BULLETIN (SB26-125)

VULNERABILITY SUMMARY FOR THE WEEK OF

**27TH APRIL, 2026**

# Bulletin (SB26-125)
# Vulnerability Summary for the Week of April 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 |
|---|---|---|---|---|
| @fedify--fedify | Fedify is a TypeScript library for building federated server apps powered by ActivityPub. Prior to 1.9.6, 1.10.5, 2.0.8, and 2.1.1, @fedify/fedify follows HTTP redirects recursively in its remote document loader and authenticated document loader without enforcing a maximum redirect count or visited-URL loop detection. An attacker who controls a remote ActivityPub key or actor URL can force a server using Fedify to make repeated outbound requests from a single inbound request, leading to resource consumption and denial of service. This vulnerability is fixed in 1.9.6, 1.10.5, 2.0.8, and 2.1.1. | 2026-04-06 | 7.5 | CVE-2026-34148 |
| AcademySoftware Foundation--openexr | OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. From 3.2.0 to before 3.2.7, 3.3.9, and 3.4.9, a misaligned memory write vulnerability exists in LossyDctDecoder_execute() in src/lib/OpenEXRCore/internal_dwa_decoder.h:749. When decoding a DWA or DWAB-compressed EXR file containing a FLOAT-type channel, the decoder performs an in-place HALF→FLOAT conversion by casting an unaligned uint8_t * row pointer to float * and writing through it. Because the row buffer may not be 4-byte aligned, this constitutes undefined behavior under the C standard and crashes immediately on architectures that enforce alignment (ARM, RISC-V, etc.). On x86 it is silently tolerated at runtime but remains exploitable via compiler optimizations that assume aligned access. This vulnerability is fixed in 3.2.7, 3.3.9, and 3.4.9. | 2026-04-06 | 7.1 | CVE-2026-34379 |
| aces--Loris | LORIS (Longitudinal Online Research and Imaging System) is a self-hosted web application that provides data- and project-management for neuroimaging research. Prior to 27.0.3 and 28.0.1, a SQL injection has been identified in some code sections for the MRI feedback popup window of the imaging browser. Attackers can use SQL ingestion to access/alter data on the server. This vulnerability is fixed in 27.0.3 and 28.0.1. | 2026-04-08 | 7.5 | CVE-2026-33350 |
| aces--Loris | LORIS (Longitudinal Online Research and Imaging System) is a self-hosted web application that provides data- and project-management for neuroimaging research. From 20.0.0 to before 27.0.3 and 28.0.1, a bug in the static file router can allow an attacker to traverse outside of the intended directory, allowing unintended files to be downloaded through the static, css, and js endpoints. This vulnerability is fixed in 27.0.3 and 28.0.1. | 2026-04-08 | 7.5 | CVE-2026-34392 |
| Across--DR-810 | Across DR-810 contains an unauthenticated file disclosure vulnerability that allows remote attackers to download the rom-0 backup file containing sensitive information by sending a simple GET request. Attackers can access the rom-0 endpoint without authentication to retrieve and decompress the backup file, exposing router passwords and other sensitive configuration data. | 2026-04-12 | 7.5 | CVE-2019-25706 |
| adianti--Adianti Framework | Adianti Framework 5.5.0 and 5.6.0 contains an SQL injection vulnerability that allows authenticated users to manipulate database queries by injecting SQL code through the name field in SystemProfileForm. Attackers can submit crafted SQL statements in the profile edit endpoint to modify user credentials and gain administrative access. | 2026-04-12 | 7.1 | CVE-2018-25257 |
| Adivaha--WordPress adivaha Travel Plugin | WordPress adivaha Travel Plugin 2.3 contains a time-based blind SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'pid' GET parameter. Attackers can send requests to the /mobile-app/v3/ endpoint with crafted 'pid' values using XOR-based payloads to extract sensitive database information or cause denial of service. | 2026-04-09 | 8.2 | CVE-2023-54359 |
| Adobe--Acrobat Reader | Acrobat Reader versions 24.001.30356, 26.001.21367 and earlier are affected by an Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') 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. | 2026-04-11 | 8.6 | CVE-2026-34621 |
| Analytify--Simple Social Media Share Buttons | Cross-Site Request Forgery (CSRF) vulnerability in Analytify Simple Social Media Share Buttons allows Cross Site Request Forgery.This issue affects Simple Social Media Share Buttons: from n/a through 6.2.0. | 2026-04-07 | 7.5 | CVE-2026-34904 |
| Analytify--Under Construction, Coming Soon & Maintenance Mode | Cross-Site Request Forgery (CSRF) vulnerability in Analytify Under Construction, Coming Soon & Maintenance Mode allows Cross Site Request Forgery.This issue affects Under Construction, Coming Soon & Maintenance Mode: from n/a through 2.1.1. | 2026-04-07 | 7.5 | CVE-2026-34896 |
| Beijing Topsec Network Security Technology Co., Ltd.--Tianxin | Tianxin Internet Behavior Management System contains a command injection vulnerability in the Reporter component endpoint that allows unauthenticated attackers to execute arbitrary commands by supplying a crafted objClass parameter containing shell metacharacters and output redirection. Attackers can | 2026-04-07 | 9.8 | CVE-2021-4473 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Internet Behavior Management System | exploit this vulnerability to write malicious PHP files into the web root and achieve remote code execution with the privileges of the web server process. This vulnerability has been fixed in version NACFirmware_4.0.0.7_20210716.180815_topsec_0_basic.bin. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-06-01 (UTC). | | | |
| CactusThemes--VideoPro | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CactusThemes VideoPro allows PHP Local File Inclusion.This issue affects VideoPro: from n/a through 2.3.8.1. | 2026-04-10 | 8.1 | CVE-2025-58913 |
| Canonical--lxd | Canonical LXD versions 4.12 through 6.7 contain an incomplete denylist in isVMLowLevelOptionForbidden (lxd/project/limits/permissions.go), which omits raw.apparmor and raw.qemu.conf from the set of keys blocked under the restricted.virtual-machines.lowlevel=block project restriction. A remote attacker with can_edit permission on a VM instance in a restricted project can inject an AppArmor rule and a QEMU chardev configuration that bridges the LXD Unix socket into the guest VM, enabling privilege escalation to LXD cluster administrator and subsequently to host root. | 2026-04-09 | 9.1 | CVE-2026-34177 |
| Canonical--lxd | In Canonical LXD before 6.8, the backup import path validates project restrictions against backup/index.yaml in the supplied tar archive but creates the instance from backup/container/backup.yaml, a separate file in the same archive that is never checked against project restrictions. An authenticated remote attacker with instance-creation permission in a restricted project can craft a backup archive where backup.yaml carries restricted settings such as security.privileged=true or raw.lxc directives, bypassing all project restriction enforcement and allowing full host compromise. | 2026-04-09 | 9.1 | CVE-2026-34178 |
| Canonical--lxd | In Canonical LXD versions 4.12 through 6.7, the doCertificateUpdate function in lxd/certificates.go does not validate the Type field when handling PUT/PATCH requests to /1.0/certificates/{fingerprint} for restricted TLS certificate users, allowing a remote authenticated attacker to escalate privileges to cluster admin. | 2026-04-09 | 9.1 | CVE-2026-34179 |
| Case Themes--Case Theme User | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Case Themes Case Theme User allows PHP Local File Inclusion.This issue affects Case Theme User: from n/a before 1.0.4. | 2026-04-10 | 7.5 | CVE-2025-5804 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, Chamilo LMS contains an OS Command Injection vulnerability in the file move function. The move() function in fileManage.lib.php passes user-controlled path values directly into exec() shell commands without using escapeshellarg(). When a user moves a document via document.php, the move_to POST parameter - which only passes through Security::remove_XSS() (an HTML-only filter) - is concatenated directly into shell commands such as exec("mv $source $target"). By default, Chamilo allows all authenticated users to create courses (allow_users_to_create_courses = true). Any user who is a teacher in a course (including self-created courses) can move documents, making this vulnerability exploitable by any authenticated user. The attacker must first place a directory with shell metacharacters in its name on the filesystem (achievable via Course Backup Import), then move a document into that directory to trigger arbitrary command execution as the web server user (www-data). This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3. | 2026-04-10 | 9.1 | CVE-2026-32892 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, the default password reset mechanism generates tokens using sha1($email) with no random component, no expiration, and no rate limiting. An attacker who knows a user's email can compute the reset token and change the victim's password without authentication. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3. | 2026-04-10 | 9.4 | CVE-2026-33707 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38, there is a path traversal in main/exercise/savescores.php leading to arbitrary file feletion. User input from $_REQUEST['test'] is concatenated directly into filesystem path without canonicalization or traversal checks. This vulnerability is fixed in 1.11.38. | 2026-04-10 | 8.3 | CVE-2026-31939 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to .0.0-RC.3, the PlatformConfigurationController::decodeSettingArray() method uses PHP's eval() to parse platform settings from the database. An attacker with admin access (obtainable via Advisory 1) can inject arbitrary PHP code into the settings, which is then executed when any user (including unauthenticated) requests /platform-config/list. This vulnerability is fixed in 2.0.0-RC.3. | 2026-04-10 | 8.8 | CVE-2026-33618 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, in main/lp/aicc_hacp.php, user-controlled request parameters are directly used to set the PHP session ID before loading global bootstrap. This leads to session fixation. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3. | 2026-04-10 | 7.5 | CVE-2026-31940 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, Chamilo LMS contains a Server-Side Request Forgery (SSRF) vulnerability in the Social Wall feature. The endpoint read_url_with_open_graph accepts a URL from the user via the social_wall_new_msg_main POST parameter and performs two server-side HTTP requests to that URL without validating whether the target is an internal or external resource. This allows an authenticated attacker to force the server to make arbitrary HTTP requests to internal services, scan internal ports, and access cloud instance metadata. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3. | 2026-04-10 | 7.7 | CVE-2026-31941 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, an Insecure Direct Object Reference (IDOR) vulnerability in the gradebook result view page allows any authenticated teacher to delete any student's grade result across the entire platform by manipulating the delete_mark or resultdelete GET parameters. No ownership or course-scope verification is performed. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3. | 2026-04-10 | 7.1 | CVE-2026-32894 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, an Insecure Direct Object Reference (IDOR) vulnerability in the gradebook evaluation edit page allows any authenticated teacher to view and modify the settings (name, max score, weight) of evaluations belonging to any other course by manipulating the editeval GET parameter. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3. | 2026-04-10 | 7.1 | CVE-2026-32930 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, an unrestricted file upload vulnerability in the exercise sound upload function allows an authenticated teacher to upload a PHP webshell by spoofing the Content-Type header to audio/mpeg. The uploaded file retains its original .php extension and is placed in a web-accessible directory, enabling Remote Code Execution as the web server user (www-data). This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3. | 2026-04-10 | 7.5 | CVE-2026-32931 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, Chamilo LMS contains an Insecure Direct Object Reference (IDOR) vulnerability in the Learning Path progress saving endpoint. The file lp_ajax_save_item.php accepts a uid (user ID) parameter directly from $_REQUEST and uses it to load and modify another user's Learning Path progress - including score, status, completion, and time - without verifying that the requesting user matches the target user ID. Any authenticated user enrolled in a course can overwrite another user's Learning Path progress by simply changing the uid parameter in the request. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3. | 2026-04-10 | 7.1 | CVE-2026-33702 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38, any authenticated user (including students) can write arbitrary content to files on the server via the BigUpload endpoint. The key parameter controls the filename and the raw POST body becomes the file content. While .php extensions are filtered to .phps, the .pht extension passes through unmodified. On Apache configurations where .pht is handled as PHP, this leads to Remote Code Execution. This vulnerability is fixed in 1.11.38. | 2026-04-10 | 7.1 | CVE-2026-33704 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38, any authenticated user with a REST API key can modify their own status field via the update_user_from_username endpoint. A student (status=5) can change their status to Teacher/CourseManager (status=1), gaining course creation and management privileges. This vulnerability is fixed in 1.11.38. | 2026-04-10 | 7.1 | CVE-2026-33706 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, REST API keys are generated using md5(time() + (user_id * 5) - rand(10000, 10000)). The rand(10000, 10000) call always returns exactly 10000 (min == max), making the formula effectively md5(timestamp + user_id*5 - 10000). An attacker who knows a username and approximate key creation time can brute-force the API key. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3. | 2026-04-10 | 7.5 | CVE-2026-33710 |
| chartbrew--chartbrew | Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to 4.9.0, a cross-tenant authorization bypass exists in Chartbrew in GET /team/:team_id/template/generate/:project_id. The GET handler calls checkAccess(req, "updateAny", "chart") without awaiting the returned promise, and it does not verify that the supplied project_id belongs to req.params.team_id or to the caller's team. As a result, an authenticated attacker with valid template-generation permissions in their own team can request the template model for a project belonging to another team and receive victim project data. This vulnerability is fixed in 4.9.0. | 2026-04-10 | 7.7 | CVE-2026-32252 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Contemporary Controls--BASControl20 | An attacker could use data obtained by sniffing the network traffic to forge packets in order to make arbitrary requests to Contemporary Controls BASC 20T. | 2026-04-09 | 9.8 | CVE-2025-13926 |
| CouchCMS--CouchCMS | CouchCMS contains a privilege escalation vulnerability that allows authenticated Admin-level users to create SuperAdmin accounts by tampering with the f_k_levels_list parameter in user creation requests. Attackers can modify the parameter value from 4 to 10 in the HTTP request body to bypass authorization validation and gain full application control, circumventing restrictions on SuperAdmin account creation and privilege assignment. | 2026-04-10 | 7.2 | CVE-2026-29002 |
| danbilabs--Advanced Members for ACF | The Advanced Members for ACF plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the create_crop function in all versions up to, and including, 1.2.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). The vulnerability was partially patched in version 1.2.5. | 2026-04-08 | 8.8 | CVE-2026-3243 |
| David Lingren--Media LIbrary Assistant | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in David Lingren Media LIbrary Assistant allows SQL Injection.This issue affects Media LIbrary Assistant: from n/a through 3.34. | 2026-04-06 | 8.5 | CVE-2026-34885 |
| davidfcarr--Quick Playground | The Quick Playground plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.3.1. This is due to insufficient authorization checks on REST API endpoints that expose a sync code and allow arbitrary file uploads. This makes it possible for unauthenticated attackers to retrieve the sync code, upload PHP files with path traversal, and achieve remote code execution on the server. | 2026-04-09 | 9.8 | CVE-2026-1830 |
| Davidtavarez--CF Image Hosting Script | CF Image Hosting Script 1.6.5 allows unauthenticated attackers to download and decode the application database by accessing the imgdb.db file in the upload/data directory. Attackers can extract delete IDs stored in plaintext from the deserialized database and use them to delete all pictures via the d parameter. | 2026-04-12 | 9.8 | CVE-2019-25709 |
| Dell--Elastic Cloud Storage | Dell Elastic Cloud Storage, version 3.8.1.7 and prior, and Dell ObjectScale, versions prior to 4.1.0.3 and version 4.2.0.0, contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to secret exposure. The attacker may be able to use the exposed secret to access the vulnerable system with privileges of the compromised account. | 2026-04-08 | 7.8 | CVE-2026-28261 |
| distribution--distribution | Distribution is a toolkit to pack, ship, store, and deliver container content. Prior to 3.1.0, in pull-through cache mode, distribution discovers token auth endpoints by parsing WWW-Authenticate challenges returned by the configured upstream registry. The realm URL from a bearer challenge is used without validating that it matches the upstream registry host. As a result, an attacker-controlled upstream (or an attacker with MitM position to the upstream) can cause distribution to send the configured upstream credentials via basic auth to an attacker-controlled realm URL. This vulnerability is fixed in 3.1.0. | 2026-04-06 | 7.5 | CVE-2026-33540 |
| Divxtodvd--Easy Video to iPod Converter | Easy Video to iPod Converter 1.6.20 contains a local buffer overflow vulnerability in the user registration field that allows local attackers to overwrite the structured exception handler. Attackers can input a crafted payload exceeding 996 bytes in the username field to trigger SEH overwrite and execute arbitrary code with user privileges. | 2026-04-12 | 8.4 | CVE-2019-25701 |
| Dolibarr--Dolibarr ERP-CRM | Dolibarr ERP-CRM 8.0.4 contains an SQL injection vulnerability in the rowid parameter of the admin dict.php endpoint that allows attackers to execute arbitrary SQL queries. Attackers can inject malicious SQL code through the rowid POST parameter to extract sensitive database information using error-based SQL injection techniques. | 2026-04-12 | 8.2 | CVE-2019-25710 |
| Dolibarr--Dolibarr ERP/CRM | Dolibarr ERP/CRM versions prior to 23.0.2 contain an authenticated remote code execution vulnerability in the dol_eval_standard() function that fails to apply forbidden string checks in whitelist mode and does not detect PHP dynamic callable syntax. Attackers with administrator privileges can inject malicious payloads through computed extrafields or other evaluation paths using PHP dynamic callable syntax to bypass validation and achieve arbitrary command execution via eval(). | 2026-04-07 | 7.2 | CVE-2026-22666 |
| Ebrigade--eBrigade ERP | eBrigade ERP 4.5 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'id' parameter. Attackers can send GET requests to pdf.php with crafted SQL payloads in the 'id' parameter to extract sensitive database information including table names and schema details. | 2026-04-12 | 7.1 | CVE-2019-25707 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Elastic--Kibana | Incorrect Authorization (CWE-863) in Kibana can lead to information disclosure via Privilege Abuse (CAPEC-122). A user with limited Fleet privileges can exploit an internal API endpoint to retrieve sensitive configuration data, including private keys and authentication tokens, that should only be accessible to users with higher-level settings privileges. The endpoint composes its response by fetching full configuration objects and returning them directly, bypassing the authorization checks enforced by the dedicated settings APIs. | 2026-04-08 | 7.7 | CVE-2026-33461 |
| Elastic--Logstash | Improper Limitation of a Pathname to a Restricted Directory (CWE-22) in Logstash can lead to arbitrary file write and potentially remote code execution via Relative Path Traversal (CAPEC-139). The archive extraction utilities used by Logstash do not properly validate file paths within compressed archives. An attacker who can serve a specially crafted archive to Logstash through a compromised or attacker-controlled update endpoint can write arbitrary files to the host filesystem with the privileges of the Logstash process. In certain configurations where automatic pipeline reloading is enabled, this can be escalated to remote code execution. | 2026-04-08 | 8.1 | CVE-2026-33466 |
| Faleemi--Faleemi Desktop Software | Faleemi Desktop Software 1.8 contains a local buffer overflow vulnerability in the System Setup dialog that allows attackers to bypass DEP protections through structured exception handling exploitation. Attackers can inject a crafted payload into the Save Path for Snapshot and Record file field to trigger a buffer overflow and execute arbitrary code via ROP chain gadgets. | 2026-04-12 | 8.4 | CVE-2019-25691 |
| GitLab--GitLab | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 13.0 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that could have allowed an unauthenticated user to cause denial of service by sending repeated GraphQL queries. | 2026-04-08 | 7.5 | CVE-2025-12664 |
| GitLab--GitLab | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.10 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that could have allowed an unauthenticated user to cause denial of service due to improper input validation of JSON payloads. | 2026-04-08 | 7.5 | CVE-2026-1092 |
| glpi-project--glpi | GLPI is a free asset and IT management software package. From 10.0.0 to before 10.0.24 and 11.0.6, an authenticated user can perform a SQL injection via the logs export feature. This vulnerability is fixed in 10.0.24 and 11.0.6. | 2026-04-06 | 7.2 | CVE-2026-29047 |
| go-vikunja--vikunja | Vikunja is an open-source self-hosted task management platform. Prior to 2.3.0, the OIDC callback handler issues a full JWT token without checking whether the matched user has TOTP two-factor authentication enabled. When a local user with TOTP enrolled is matched via the OIDC email fallback mechanism, the second factor is completely skipped. This vulnerability is fixed in 2.3.0. | 2026-04-10 | 7.4 | CVE-2026-34727 |
| HDFGroup--hdf5 | HDF5 is software for managing data. In 1.14.1-2 and earlier, a heap-use-after-free was found in the h5dump helper utility. An attacker who can supply a malicious h5 file can trigger a heap use-after-free. The freed object is referenced in a memmove call from H5T__conv_struct. The original object was allocated by H5D__typeinfo_init_phase3 and freed by H5D__typeinfo_term. | 2026-04-09 | 7.8 | CVE-2026-34734 |
| Hitachi--JP1/IT Desktop Management 2 - Manager | Remote Code Execution Vulnerability in JP1/IT Desktop Management 2 - Manager on Windows, JP1/IT Desktop Management 2 - Operations Director on Windows, Job Management Partner 1/IT Desktop Management 2 - Manager on Windows, JP1/IT Desktop Management - Manager on Windows, Job Management Partner 1/IT Desktop Management - Manager on Windows, JP1/NETM/DM Manager on Windows, JP1/NETM/DM Client on Windows, Job Management Partner 1/Software Distribution Manager on Windows, Job Management Partner 1/Software Distribution Client on Windows.This issue affects JP1/IT Desktop Management 2 - Manager: from 13-50 before 13-50-02, from 13-11 before 13-11-04, from 13-10 before 13-10-07, from 13-01 before 13-01-07, from 13-00 before 13-00-05, from 12-60 before 12-60-12, from 10-50 through 12-50-11; JP1/IT Desktop Management 2 - Operations Director: from 13-50 before 13-50-02, from 13-11 before 13-11-04, from 13-10 before 13-10-07, from 13-01 before 13-01-07, from 13-00 before 13-00-05, from 12-60 before 12-60-12, from 10-50 through 12-50-11; Job Management Partner 1/IT Desktop Management 2 - Manager: from 10-50 through 10-50-11; JP1/IT Desktop Management - Manager: from 09-50 through 10-10-16; Job Management Partner 1/IT Desktop Management - Manager: from 09-50 through 10-10-16; JP1/NETM/DM Manager: from 09-00 through 10-20-02; JP1/NETM/DM Client: from 09-00 through 10-20-02; Job Management Partner 1/Software Distribution Manager: from 09-00 through 09-51-13; Job Management Partner 1/Software Distribution Client: from 09-00 through 09-51-13. | 2026-04-07 | 8.8 | CVE-2025-65115 |
| HKUDS--OpenHarness | OpenHarness prior to commit 166fcfe contains an improper access control vulnerability in built-in file tools due to inconsistent parameter handling in permission enforcement, allowing attackers who can influence agent tool | 2026-04-07 | 7.1 | CVE-2026-22682 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | execution to read arbitrary local files outside the intended repository scope. Attackers can exploit the path parameter not being passed to the PermissionChecker in read_file, write_file, edit_file, and notebook_edit tools to bypass deny rules and access sensitive files such as configuration files, credentials, and SSH material, or create and overwrite files in restricted host paths in full_auto mode. | | | |
| homarr-labs--homarr | Homarr is an open-source dashboard. Prior to 1.57.0, a DOM-based Cross-Site Scripting (XSS) vulnerability has been discovered in Homarr's /auth/login page. The application improperly trusts a URL parameter (callbackUrl), which is passed to redirect and router.push. An attacker can craft a malicious link that, when opened by an authenticated user, performs a client-side redirect and executes arbitrary JavaScript in the context of their browser. This could lead to credential theft, internal network pivoting, and unauthorized actions performed on behalf of the victim. This vulnerability is fixed in 1.57.0. | 2026-04-06 | 8.8 | CVE-2026-33510 |
| Html5Videoplayer--HTML5 Video Player | HTML5 Video Player 1.2.5 contains a local buffer overflow vulnerability that allows attackers to execute arbitrary code by supplying an oversized key code string. Attackers can craft a malicious payload exceeding 997 bytes and paste it into the KEY CODE field in the Help Register dialog to trigger code execution and spawn a calculator process. | 2026-04-12 | 8.4 | CVE-2019-25689 |
| IBM--Langflow Desktop | IBM Langflow Desktop 1.6.0 through 1.8.2 Langflow could allow an authenticated user to execute arbitrary code on the system, caused by an insecure default setting which permits the deserialization of untrusted data in the FAISS component. | 2026-04-08 | 8.8 | CVE-2026-3357 |
| IBM--Verify Identity Access Container | IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 could allow a locally authenticated user to escalate their privileges to root due to execution with unnecessary privileges than required. | 2026-04-08 | 9.3 | CVE-2026-1346 |
| IBM--Verify Identity Access Container | IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 could allow a locally authenticated user to execute malicious scripts from outside of its control sphere. | 2026-04-07 | 8.5 | CVE-2026-1342 |
| IBM--Verify Identity Access Container | IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 allows an attacker to contact internal authentication endpoints which are protected by the Reverse Proxy. | 2026-04-08 | 7.2 | CVE-2026-1343 |
| Impresscms--ImpressCMS | ImpressCMS 1.3.11 contains a time-based blind SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the 'bid' parameter. Attackers can send POST requests to the admin.php endpoint with malicious 'bid' values containing SQL commands to extract sensitive database information. | 2026-04-12 | 7.1 | CVE-2019-25703 |
| Juniper Networks--Apstra | A Key Exchange without Entity Authentication vulnerability in the SSH implementation of Juniper Networks Apstra allows a unauthenticated, MITM attacker to impersonate managed devices. Due to insufficient SSH host key validation an attacker can perform a machine-in-the-middle attack on the SSH connections from Apstra to managed devices, enabling an attacker to impersonate a managed device and capture user credentials. This issue affects all versions of Apstra before 6.1.1. | 2026-04-09 | 8.7 | CVE-2025-13914 |
| Juniper Networks--CTP OS | A Weak Password Requirements vulnerability in the password management function of Juniper Networks CTP OS might allow an unauthenticated, network-based attacker to exploit weak passwords of local accounts and potentially take full control of the device. The password management menu enables the administrator to set password complexity requirements, but these settings are not saved. The issue can be verified with the menu option "Show password requirements". Failure to enforce the intended requirements can lead to weak passwords being used, which significantly increases the likelihood that an attacker can guess these and subsequently attain unauthorized access. This issue affects CTP OS versions 9.2R1 and 9.2R2. | 2026-04-09 | 7.4 | CVE-2026-33771 |
| Juniper Networks--JSI LWC | A Use of Default Password vulnerability in the Juniper Networks Support Insights (JSI) Virtual Lightweight Collector (vLWC) allows an unauthenticated, network-based attacker to take full control of the device. vLWC software images ship with an initial password for a high privileged account. A change of this password is not enforced during the provisioning of the software, which can make full access to the | 2026-04-09 | 9.8 | CVE-2026-33784 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | system by unauthorized actors possible.This issue affects all versions of vLWC before 3.0.94. | | | |
| Juniper Networks--Junos OS | A Missing Authorization vulnerability in the CLI of Juniper Networks Junos OS on MX Series allows a local, authenticated user with low privileges to execute specific commands which will lead to a complete compromise of managed devices. Any user logged in, without requiring specific privileges, can issue 'request csds' CLI operational commands. These commands are only meant to be executed by high privileged or users designated for Juniper Device Manager (JDM) / Connected Security Distributed Services (CSDS) operations as they will impact all aspects of the devices managed via the respective MX. This issue affects Junos OS on MX Series: * 24.4 releases before 24.4R2-S3, * 25.2 releases before 25.2R2. This issue does not affect Junos OS releases before 24.4. | 2026-04-09 | 8.8 | CVE-2026-33785 |
| Juniper Networks--Junos OS | A UNIX Symbolic Link (Symlink) Following vulnerability in the CLI of Juniper Networks Junos OS allows a local, authenticated attacker with low privileges to escalate their privileges to root which will lead to a complete compromise of the system. When after a user has performed a specific 'file link ...' CLI operation, another user commits (unrelated configuration changes), the first user can login as root. This issue affects Junos OS: * 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-S2, * 25.2 versions before 25.2R2. This issue does not affect versions 25.4R1 or later. | 2026-04-09 | 7.3 | CVE-2026-21916 |
| Juniper Networks--Junos OS | An Improper Validation of Syntactic Correctness of Input vulnerability in the IPsec library used by kmd and iked of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a complete Denial-of-Service (DoS). If an affected device receives a specifically malformed first ISAKMP packet from the initiator, the kmd/iked process will crash and restart, which momentarily prevents new security associations (SAs) for from being established. Repeated exploitation of this vulnerability causes a complete inability to establish new VPN connections. This issue affects Junos OS on SRX Series and MX Series: * all versions before 22.4R3-S9, * 23.2 version before 23.2R2-S6, * 23.4 version before 23.4R2-S7, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S3, * 25.2 versions before 25.2R1-S2, 25.2R2. | 2026-04-09 | 7.5 | CVE-2026-33778 |
| Juniper Networks--Junos OS | An Improper Check for Unusual or Exceptional Conditions vulnerability in the flow daemon (flowd) of Juniper Networks Junos OS on SRX Series allows an attacker sending a specific, malformed ICMPv6 packet to cause the srxpfe process to crash and restart. Continued receipt and processing of these packets will repeatedly crash the srxpfe process and sustain the Denial of Service (DoS) condition. During NAT64 translation, receipt of a specific, malformed ICMPv6 packet destined to the device will cause the srxpfe process to crash and restart. This issue cannot be triggered using IPv4 nor other IPv6 traffic. This issue affects Junos OS on SRX Series: * all versions before 21.2R3-S10, * all versions of 21.3, * from 21.4 before 21.4R3-S12, * all versions of 22.1, * from 22.2 before 22.2R3-S8, * all versions of 22.4, * from 22.4 before 22.4R3-S9, * from 23.2 before 23.2R2-S6, * from 23.4 before 23.4R2-S7, * from 24.2 before 24.2R2-S3, * from 24.4 before 24.4R2-S3, * from 25.2 before 25.2R1-S2, 25.2R2. | 2026-04-09 | 7.5 | CVE-2026-33790 |
| Juniper Networks--Junos OS | An Execution with Unnecessary Privileges vulnerability in the User Interface (UI) of Juniper Networks Junos OS and Junos OS Evolved allows a local, low-privileged attacker to gain root privileges, thus compromising the system. When a configuration that allows unsigned Python op scripts is present on the device, a non-root user is able to execute malicious op scripts as a root-equivalent user, leading to privilege escalation. This issue affects Junos OS: * All versions before 22.4R3-S7, * from 23.2 before 23.2R2-S4, * from 23.4 before 23.4R2-S6, * from 24.2 before 24.2R1-S2, 24.2R2, * from 24.4 before 24.4R1-S2, 24.4R2; Junos OS Evolved: * All versions before 22.4R3-S7-EVO, * from 23.2 before 23.2R2-S4-EVO, * from 23.4 before 23.4R2-S6-EVO, * from 24.2 before 24.2R2-EVO, * from 24.4 before 24.4R1-S1-EVO, 24.4R2-EVO. | 2026-04-09 | 7.8 | CVE-2026-33793 |
| Juniper Networks--Junos OS | An Improper Input Validation vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker, sending a specific genuine BGP packet in an already established BGP session to reset only that session causing a Denial of Service (DoS). An attacker repeatedly sending the packet will sustain the Denial of Service (DoS).This issue affects Junos OS: * 25.2 versions before 25.2R2 This issue doesn't not affected Junos OS versions before 25.2R1. This issue affects Junos OS Evolved: * 25.2-EVO versions before 25.2R2-EVO This issue doesn't not affected Junos OS Evolved versions before 25.2R1-EVO. eBGP and iBGP are affected. IPv4 and IPv6 are affected. | 2026-04-09 | 7.4 | CVE-2026-33797 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Juniper Networks--Junos OS Evolved | A Missing Authentication for Critical Function vulnerability in the Flexible PIC Concentrators (FPCs) of Juniper Networks Junos OS Evolved on PTX Series allows a local, authenticated attacker with low privileges to gain direct access to FPCs installed in the device. A local user with low privileges can gain direct access to the installed FPCs as a high privileged user, which can potentially lead to a full compromise of the affected component. This issue affects Junos OS Evolved on PTX10004, PTX10008, PTX100016, with JNP10K-LC1201 or JNP10K-LC1202: * All versions before 21.2R3-S8-EVO, * 21.4-EVO versions before 21.4R3-S7-EVO, * 22.2-EVO versions before 22.2R3-S4-EVO, * 22.3-EVO versions before 22.3R3-S3-EVO, * 22.4-EVO versions before 22.4R3-S2-EVO, * 23.2-EVO versions before 23.2R2-EVO. | 2026-04-09 | 7.8 | CVE-2026-33788 |
| lexiforest--curl_cffi | curl_cffi is the a Python binding for curl. Prior to 0.15.0, curl_cffi does not restrict requests to internal IP ranges, and follows redirects automatically via the underlying libcurl. Because of this, an attacker-controlled URL can redirect requests to internal services such as cloud metadata endpoints. In addition, curl_cffi's TLS impersonation feature can make these requests appear as legitimate browser traffic, which may bypass certain network controls. This vulnerability is fixed in 0.15.0. | 2026-04-06 | 8.6 | CVE-2026-33752 |
| LibRaw--LibRaw | A heap-based buffer overflow vulnerability exists in the x3f_thumb_loader functionality of LibRaw Commit d20315b. A specially crafted malicious file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability. | 2026-04-07 | 9.8 | CVE-2026-20889 |
| LibRaw--LibRaw | A heap-based buffer overflow vulnerability exists in the HuffTable::initval functionality of LibRaw Commit 0b56545 and Commit d20315b. A specially crafted malicious file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability. | 2026-04-07 | 9.8 | CVE-2026-20911 |
| LibRaw--LibRaw | A heap-based buffer overflow vulnerability exists in the lossless_jpeg_load_raw functionality of LibRaw Commit 0b56545 and Commit d20315b. A specially crafted malicious file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability. | 2026-04-07 | 9.8 | CVE-2026-21413 |
| LibRaw--LibRaw | An integer overflow vulnerability exists in the deflate_dng_load_raw functionality of LibRaw Commit 8dc68e2. A specially crafted malicious file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability. | 2026-04-07 | 8.1 | CVE-2026-20884 |
| MontFerret--ferret | Ferret is a declarative system for working with web data. Prior to 2.0.0-alpha.4, a path traversal vulnerability in Ferret's IO::FS::WRITE standard library function allows a malicious website to write arbitrary files to the filesystem of the machine running Ferret. When an operator scrapes a website that returns filenames containing ../ sequences, and uses those filenames to construct output paths (a standard scraping pattern), the attacker controls both the destination path and the file content. This can lead to remote code execution via cron jobs, SSH authorized_keys, shell profiles, or web shells. This vulnerability is fixed in 2.0.0-alpha.4. | 2026-04-06 | 8.1 | CVE-2026-34783 |
| MyT--Project Management | MyT-PM 1.5.1 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the Charge[group_total] parameter. Attackers can submit crafted POST requests to the /charge/admin endpoint with error-based, time-based blind, or stacked query payloads to extract sensitive database information or manipulate data. | 2026-04-12 | 7.1 | CVE-2019-25713 |
| Newsbull--Newsbull Haber Script | Newsbull Haber Script 1.0.0 contains multiple SQL injection vulnerabilities in the search parameter that allow authenticated attackers to extract database information through time-based, blind, and boolean-based injection techniques. Attackers can inject malicious SQL code through the search parameter in endpoints like /admin/comment/records, /admin/category/records, /admin/news/records, and /admin/menu/childs to manipulate database queries and retrieve sensitive data. | 2026-04-12 | 7.1 | CVE-2019-25699 |
| Nextendweb--Smart Slider 3 Pro for WordPress | Smart Slider 3 Pro version 3.5.1.35 for WordPress and Joomla contains a multi-stage remote access toolkit injected through a compromised update system that allows unauthenticated attackers to execute arbitrary code and commands. Attackers can trigger pre-authentication remote shell execution via HTTP headers, establish authenticated backdoors accepting arbitrary PHP code or OS commands, create hidden administrator accounts, exfiltrate credentials and access keys, and maintain persistence through multiple injection points including must-use plugins and core file modifications. | 2026-04-09 | 9.8 | CVE-2026-34424 |
| NI--LabVIEW | There is a memory corruption vulnerability due to an out-of-bounds write when loading a corrupted LVLIB file in NI LabVIEW. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires | 2026-04-07 | 7.8 | CVE-2026-32860 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | an attacker to get a user to open a specially crafted .lvlib file. This vulnerability affects NI LabVIEW 2026 Q1 (26.1.0) and prior versions. | | | |
| NI--LabVIEW | There is a memory corruption vulnerability due to an out-of-bounds write when loading a corrupted LVCLASS file in NI LabVIEW. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted .lvclass file. This vulnerability affects NI LabVIEW 2026 Q1 (26.1.0) and prior versions. | 2026-04-07 | 7.8 | CVE-2026-32861 |
| NI--LabVIEW | There is a memory corruption vulnerability due to an out-of-bounds write in ResFileFactory::InitResourceMgr() in NI LabVIEW. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI file. This vulnerability affects NI LabVIEW 2026 Q1 (26.1.0) and prior versions. | 2026-04-07 | 7.8 | CVE-2026-32862 |
| NI--LabVIEW | There is a memory corruption vulnerability due to an out-of-bounds read in sentry_transaction_context_set_operation() in NI LabVIEW. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI file. This vulnerability affects NI LabVIEW 2026 Q1 (26.1.0) and prior versions. | 2026-04-07 | 7.8 | CVE-2026-32863 |
| NI--LabVIEW | There is a memory corruption vulnerability due to an out-of-bounds read in mgcore_SH_25_3!aligned_free() in NI LabVIEW. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI file. This vulnerability affects NI LabVIEW 2026 Q1 (26.1.0) and prior versions. | 2026-04-07 | 7.8 | CVE-2026-32864 |
| nyariv--SandboxJS | SandboxJS is a JavaScript sandboxing library. Prior to 0.8.36, SandboxJS blocks direct assignment to global objects (for example Math.random = ...), but this protection can be bypassed through an exposed callable constructor path: this.constructor.call(target, attackerObject). Because this.constructor resolves to the internal SandboxGlobal function and Function.prototype.call is allowed, attacker code can write arbitrary properties into host global objects and persist those mutations across sandbox instances in the same process. This vulnerability is fixed in 0.8.36. | 2026-04-06 | 10 | CVE-2026-34208 |
| open-telemetry--opentelemetry-go | OpenTelemetry-Go is the Go implementation of OpenTelemetry. From 1.36.0 to 1.40.0, multi-value baggage: header extraction parses each header field-value independently and aggregates members across values. This allows an attacker to amplify cpu and allocations by sending many baggage: header lines, even when each individual value is within the 8192-byte per-value parse limit. This vulnerability is fixed in 1.41.0. | 2026-04-07 | 7.5 | CVE-2026-29181 |
| OpenClaw--OpenClaw | OpenClaw before 2026.3.25 contains an improper access control vulnerability in the HTTP /sessions/:sessionKey/kill route that allows any bearer-authenticated user to invoke admin-level session termination functions without proper scope validation. Attackers can exploit this by sending authenticated requests to kill arbitrary subagent sessions via the killSubagentRunAdmin function, bypassing ownership and operator scope restrictions. | 2026-04-09 | 8.1 | CVE-2026-34512 |
| opnsense--core | OPNsense is a FreeBSD based firewall and routing platform. Prior to 26.1.6, OPNsense's LDAP authentication connector passes the login username directly into an LDAP search filter without calling ldap_escape(). An unauthenticated attacker can inject LDAP filter metacharacters into the username field of the WebGUI login page to enumerate valid LDAP usernames in the configured directory. When the LDAP server configuration includes an Extended Query to restrict login to members of a specific group, the same injection can be used to bypass that group membership restriction and authenticate as any LDAP user whose password is known, regardless of group membership. This vulnerability is fixed in 26.1.6. | 2026-04-09 | 8.2 | CVE-2026-34578 |
| podman-desktop--podman-desktop | Podman Desktop is a graphical tool for developing on containers and Kubernetes. Prior to 1.26.2, an unauthenticated HTTP server exposed by Podman Desktop allows any network attacker to remotely trigger denial-of-service conditions and extract sensitive information. By abusing missing connection limits and timeouts, an attacker can exhaust file descriptors and kernel memory, leading to application crash or full host freeze. Additionally, verbose error responses disclose internal paths and system details (including usernames on Windows), aiding further exploitation. The issue requires no authentication or user interaction and is exploitable over the network. This vulnerability is fixed in 1.26.2. | 2026-04-07 | 8.2 | CVE-2026-34045 |
| prosolution--ProSolution WP Client | The ProSolution WP Client plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'proSol_fileUploadProcess' function in all versions up to, and including, 1.9.9. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. | 2026-04-08 | 9.8 | CVE-2026-2942 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Qualcomm, Inc.--Snapdragon | Memory corruption when decoding corrupted satellite data files with invalid signature offsets. | 2026-04-06 | 8.8 | CVE-2025-47392 |
| Qualcomm, Inc.--Snapdragon | Memory corruption when buffer copy operation fails due to integer overflow during attestation report generation. | 2026-04-06 | 7.8 | CVE-2025-47389 |
| Qualcomm, Inc.--Snapdragon | Memory corruption while preprocessing IOCTL request in JPEG driver. | 2026-04-06 | 7.8 | CVE-2025-47390 |
| Qualcomm, Inc.--Snapdragon | Memory corruption while processing a frame request from user. | 2026-04-06 | 7.8 | CVE-2025-47391 |
| Qualcomm, Inc.--Snapdragon | Cryptographic issue while copying data to a destination buffer without validating its size. | 2026-04-06 | 7.1 | CVE-2025-47400 |
| Qualcomm, Inc.--Snapdragon | Transient DOS when processing nonstandard FILS Discovery Frames with out-of-range action sizes during initial scans. | 2026-04-06 | 7.6 | CVE-2026-21367 |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when retrieving output buffer with insufficient size validation. | 2026-04-06 | 7.8 | CVE-2026-21371 |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when sending IOCTL requests with invalid buffer sizes during memcpy operations. | 2026-04-06 | 7.8 | CVE-2026-21372 |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when accessing an output buffer without validating its size during IOCTL processing. | 2026-04-06 | 7.8 | CVE-2026-21373 |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when processing auxiliary sensor input/output control commands with insufficient buffer size validation. | 2026-04-06 | 7.8 | CVE-2026-21374 |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when accessing an output buffer without validating its size during IOCTL processing. | 2026-04-06 | 7.8 | CVE-2026-21375 |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when accessing an output buffer without validating its size during IOCTL processing in a camera sensor driver. | 2026-04-06 | 7.8 | CVE-2026-21376 |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when accessing an output buffer without validating its size during IOCTL processing in a camera sensor driver. | 2026-04-06 | 7.8 | CVE-2026-21378 |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when using deprecated DMABUF IOCTL calls to manage video memory. | 2026-04-06 | 7.8 | CVE-2026-21380 |
| Qualcomm, Inc.--Snapdragon | Transient DOS when receiving a service data frame with excessive length during device matching over a neighborhood awareness network protocol connection. | 2026-04-06 | 7.6 | CVE-2026-21381 |
| Qualcomm, Inc.--Snapdragon | Memory Corruption when handling power management requests with improperly sized input/output buffers. | 2026-04-06 | 7.8 | CVE-2026-21382 |
| r-project--R | R 3.4.4 contains a local buffer overflow vulnerability that allows attackers to execute arbitrary code by injecting malicious input into the GUI Preferences language field. Attackers can craft a payload with a 292-byte offset and JMP ESP instruction to execute commands like calc.exe when the payload is pasted into the Language for menus and messages field. | 2026-04-12 | 8.4 | CVE-2019-25695 |
| R-Project--RGui | RGui 3.5.0 contains a local buffer overflow vulnerability in the GUI preferences dialog that allows attackers to bypass DEP protections through structured exception handling exploitation. Attackers can craft malicious input in the Language for menus and messages field to trigger a stack-based buffer overflow, execute a ROP chain for VirtualAlloc allocation, and achieve arbitrary code execution. | 2026-04-12 | 8.4 | CVE-2018-25258 |
| Red Hat--mirror registry for Red Hat OpenShift | A flaw was found in Red Hat Quay's container image upload process. An authenticated user with push access to any repository on the registry can interfere with image uploads in progress by other users, including those in repositories they do not have access to. This could allow the attacker to read, modify, or cancel another user's in-progress image upload. | 2026-04-08 | 7.1 | CVE-2026-32589 |
| Red Hat--mirror registry for Red Hat OpenShift | A flaw was found in Red Hat Quay's handling of resumable container image layer uploads. The upload process stores intermediate data in the database using a format that, if tampered with, could allow an attacker to execute arbitrary code on the Quay server. | 2026-04-08 | 7.1 | CVE-2026-32590 |
| Red Hat--Red Hat Enterprise Linux 10 | A flaw was found in libssh. This vulnerability allows local man-in-the-middle attacks, security downgrades of SSH (Secure Shell) connections, and manipulation of trusted host information, posing a significant risk to the confidentiality, integrity, and availability of SSH communications via an insecure default configuration on Windows systems where the library automatically loads configuration files from the C:\etc directory, which can be created and modified by unprivileged local users. | 2026-04-07 | 7.8 | CVE-2025-14821 |
| Red Hat--Red Hat Enterprise Linux 10 | A flaw was found in gnutls. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted ClientHello message with an invalid Pre-Shared Key (PSK) binder value during the TLS handshake. This can lead to a NULL pointer dereference, causing the server to crash and resulting in a remote Denial of Service (DoS) condition. | 2026-04-09 | 7.5 | CVE-2026-1584 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Resourcespace--ResourceSpace | ResourceSpace 8.6 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the keywords parameter in collection_edit.php. Attackers can submit POST requests with crafted SQL payloads in the keywords field to extract sensitive database information including schema names, user credentials, and other confidential data. | 2026-04-12 | 7.1 | CVE-2019-25693 |
| Rukovoditel--Rukovoditel CRM | A reflected cross-site scripting (XSS) vulnerability exists in Rukovoditel CRM version 3.6.4 and earlier in the Zadarma telephony API endpoint (/api/tel/zadarma.php). The application directly reflects user-supplied input from the 'zd_echo' GET parameter into the HTTP response without proper sanitization, output encoding, or content-type restrictions. The vulnerable code is: if (isset($_GET['zd_echo'])) exit($_GET['zd_echo']); An unauthenticated attacker can exploit this issue by crafting a malicious URL containing JavaScript payloads. When a victim visits the link, the payload executes in the context of the application within the victim's browser, potentially leading to session hijacking, credential theft, phishing, or account takeover. The issue is fixed in version 3.7, which introduces proper input validation and output encoding to prevent script injection. | 2026-04-11 | 9.3 | CVE-2026-31845 |
| saleor--saleor | Saleor is an e-commerce platform. From 2.0.0 to before 3.23.0a3, 3.22.47, 3.21.54, and 3.20.118, Saleor supports query batching by submitting multiple GraphQL operations in a single HTTP request as a JSON array but wasn't enforcing any upper limit on the number of operations. This allowed an unauthenticated attacker to send a single HTTP request many operations (bypassing the per query complexity limit) to exhaust resources. This vulnerability is fixed in 3.23.0a3, 3.22.47, 3.21.54, and 3.20.118. | 2026-04-08 | 7.5 | CVE-2026-33756 |
| SaturdayDrive--Ninja Forms - File Uploads | The Ninja Forms - File Uploads plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'NF_FU_AJAX_Controllers_Uploads::handle_upload' function in all versions up to, and including, 3.3.26. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. Note: The vulnerability was partially patched in version 3.3.25 and fully patched in version 3.3.27. | 2026-04-07 | 9.8 | CVE-2026-0740 |
| shamimmoeen--WCAPF Ajax Product Filter for WooCommerce | WCAPF - WooCommerce Ajax Product Filter plugin is vulnerable to time-based SQL Injection via the 'post-author' parameter in all versions up to, and including, 4.2.3 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. | 2026-04-08 | 7.5 | CVE-2026-3396 |
| Sourceforge--Echo Mirage | Echo Mirage 3.1 contains a stack buffer overflow vulnerability that allows local attackers to crash the application or execute arbitrary code by supplying an oversized string in the Rules action field. Attackers can create a malicious text file with a crafted payload exceeding buffer boundaries and paste it into the action field through the Rules dialog to trigger the overflow and overwrite the return address. | 2026-04-12 | 8.4 | CVE-2019-25705 |
| Synology--Synology SSL VPN Client | A plaintext storage of a password vulnerability in Synology SSL VPN Client before 1.4.5-0684 allows remote attackers to access or influence the user's PIN code due to insecure storage. This may lead to unauthorized VPN configuration and potential interception of subsequent VPN traffic when combined with user interaction. | 2026-04-10 | 8.1 | CVE-2021-47961 |
| themeum--Tutor LMS eLearning and online course solution | The Tutor LMS - eLearning and online course solution plugin for WordPress is vulnerable to an Insecure Direct Object Reference in all versions up to, and including, 3.9.7. This is due to missing authentication and authorization checks in the `pay_incomplete_order()` function. The function accepts an attacker-controlled `order_id` parameter and uses it to look up order data, then writes billing fields to the order owner's profile (`$order_data->user_id`) without verifying the requester's identity or ownership. Because the Tutor nonce (`_tutor_nonce`) is exposed on public frontend pages, this makes it possible for unauthenticated attackers to overwrite the billing profile (name, email, phone, address) of any user who has an incomplete manual order, by sending a crafted POST request with a guessed or enumerated `order_id`. | 2026-04-10 | 7.5 | CVE-2026-3360 |
| Tinyproxy Project--Tinyproxy | Tinyproxy through 1.11.3 is vulnerable to HTTP request parsing desynchronization due to a case-sensitive comparison of the Transfer-Encoding header in src/reqs.c. The is_chunked_transfer() function uses strcmp() to compare the header value against "chunked", even though RFC 7230 specifies that transfer-coding names are case-insensitive. By sending a request with Transfer-Encoding: Chunked, an unauthenticated remote attacker can cause Tinyproxy to misinterpret the request as having no body. In this state, Tinyproxy sets content_length.client to -1, skips | 2026-04-07 | 7.5 | CVE-2026-31842 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | pull_client_data_chunked(), forwards request headers upstream, and transitions into relay_connection() raw TCP forwarding while unread body data remains buffered. This leads to inconsistent request state between Tinyproxy and backend servers. RFC-compliant backends (e.g., Node.js, Nginx) will continue waiting for chunked body data, causing connections to hang indefinitely. This behavior enables application-level denial of service through backend worker exhaustion. Additionally, in deployments where Tinyproxy is used for request-body inspection, filtering, or security enforcement, the unread body may be forwarded without proper inspection, resulting in potential security control bypass. | | | |
| Twitch--Twitch Studio | Twitch Studio version 0.114.8 and prior contain a privilege escalation vulnerability in its privileged helper tool that allows local attackers to execute arbitrary code as root by exploiting an unprotected XPC service. Attackers can invoke the installFromPath:toPath:withReply: method to overwrite system files and privileged binaries, achieving full system compromise. Twitch Studio was discontinued in May 2024. | 2026-04-06 | 7.8 | CVE-2024-14032 |
| usebruno--bruno | Bruno is an open source IDE for exploring and testing APIs. Prior to 3.2.1, Bruno was affected by a supply chain attack involving compromised versions of the axios npm package, which introduced a hidden dependency deploying a cross-platform Remote Access Trojan (RAT). Users of @usebruno/cli who ran npm install between 00:21 UTC and ~03:30 UTC on March 31, 2026 may have been impacted. Upgrade to 3.2.1 | 2026-04-06 | 9.8 | CVE-2026-34841 |
| VictorAlagwu--CMSsite | CMSsite 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the cat_id parameter. Attackers can send GET requests to category.php with malicious cat_id values to extract sensitive database information including usernames and credentials. | 2026-04-12 | 8.2 | CVE-2019-25697 |
| VMware--Spring Cloud Gateway | When configuring SSL bundles in Spring Cloud Gateway by using the configuration property spring.ssl.bundle, the configuration was silently ignored and the default SSL configuration was used instead. Note: The 4.2.x branch is no longer under open source support. If you are using Spring Cloud Gateway 4.2.0 and are not an enterprise customer, you can upgrade to any Spring Cloud Gateway 4.2.x release newer than 4.2.0 available on Maven Centeral https://repo1.maven.org/maven2/org/springframework/cloud/spring-cloud-gateway/ . Ideally if you are not an enterprise customer, you should be upgrading to 5.0.2 or 5.1.1 which are the current supported open source releases. | 2026-04-10 | 7.5 | CVE-2026-22750 |
| WAGO--CC100 (0751-9x01) | An authenticated remote attacker with high privileges can exploit the OpenVPN configuration via the web-based management interface of a WAGO PLC. If user-defined scripts are permitted, OpenVPN may allow the execution of arbitrary shell commands enabling the attacker to run arbitrary commands on the device. | 2026-04-09 | 7.2 | CVE-2024-1490 |
| Weaver Network Co., Ltd.--E-cology | Weaver (Fanwei) E-cology 10.0 versions prior to 20260312 contain an unauthenticated remote code execution vulnerability in the /papi/esearch/data/devops/dubboApi/debug/method endpoint that allows attackers to execute arbitrary commands by invoking exposed debug functionality. Attackers can craft POST requests with attacker-controlled interfaceName and methodName parameters to reach command-execution helpers and achieve arbitrary command execution on the system. Exploitation evidence was first observed by the Shadowserver Foundation on 2026-03-31 (UTC). | 2026-04-07 | 9.8 | CVE-2026-22679 |
| Windmill Labs--Windmill CE (Community Edition) | Windmill versions 1.56.0 through 1.614.0 contain a missing authorization vulnerability that allows users with the Operator role to perform prohibited entity creation and modification actions via the backend API. Although Operators are documented and priced as unable to create or modify entities, the API does not enforce the Operator restriction on workspace endpoints, allowing an Operator to create and update scripts, flows, apps, and raw_apps. Since Operators can also execute scripts via the jobs API, this allows direct privilege escalation to remote code execution within the Windmill deployment. This vulnerability has existed since the introduction of the Operator role in version 1.56.0. | 2026-04-07 | 8.8 | CVE-2026-22683 |
| wpeverest--Everest Forms Contact Form, Payment Form, Quiz, Survey & Custom Form Builder | The Everest Forms plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.4.3 via deserialization of untrusted input from form entry metadata. This is due to the html-admin-page-entries-view.php file calling PHP's native unserialize() on stored entry meta values without passing the allowed_classes parameter. This makes it possible for unauthenticated attackers to inject a serialized PHP object payload through any public Everest Forms form field. The payload survives sanitize_text_field() sanitization (serialization control characters are not stripped) and is stored in the wp_evf_entrymeta database table. | 2026-04-08 | 9.8 | CVE-2026-3296 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | When an administrator views entries or views an individual entry, the unsafe unserialize() call processes the stored data without class restrictions. | | | |
| Zootemplate--Cerato | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zootemplate Cerato allows Reflected XSS.This issue affects Cerato: from n/a through 2.2.18. | 2026-04-10 | 7.1 | CVE-2025-58920 |
| Barracuda Networks--RMM | Barracuda RMM versions prior to 2025.2.2 contain a privilege escalation vulnerability that allows local attackers to gain SYSTEM-level privileges by exploiting overly permissive filesystem ACLs on the C:\Windows\Automation directory. Attackers can modify existing automation content or place attacker-controlled files in this directory, which are then executed under the NT AUTHORITY\SYSTEM account during routine automation cycles, typically succeeding within the next execution cycle. | 2026-04-15 | 7.8 | CVE-2026-22676 |
| Bosch--BVMS | Uncontrolled Resource Consumption in Bosch VMS Central Server in Bosch VMS 12.0.1 allows attackers to consume excessive amounts of disk space via network interface. | 2026-04-15 | 7.5 | CVE-2024-33618 |
| Cisco--Cisco Identity Services Engine Software | A vulnerability in Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have valid administrative credentials. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to root. In single-node ISE deployments, successful exploitation of this vulnerability could cause the affected ISE node to become unavailable, resulting in a denial of service (DoS) condition. In that condition, endpoints that have not already authenticated would be unable to access the network until the node is restored. | 2026-04-15 | 9.9 | CVE-2026-20147 |
| Cisco--Cisco Identity Services Engine Software | A vulnerability in Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have at least Read Only Admin credentials. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to root. In single-node ISE deployments, successful exploitation of these vulnerabilities could cause the affected ISE node to become unavailable, resulting in a denial of service (DoS) condition. In that condition, endpoints that have not already authenticated would be unable to access the network until the node is restored. | 2026-04-15 | 9.9 | CVE-2026-20180 |
| Cisco--Cisco Identity Services Engine Software | A vulnerability in Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have at least Read Only Admin credentials. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to root. In single-node ISE deployments, successful exploitation of these vulnerabilities could cause the affected ISE node to become unavailable, resulting in a denial of service (DoS) condition. In that condition, endpoints that have not already authenticated would be unable to access the network until the node is restored. | 2026-04-15 | 9.9 | CVE-2026-20186 |
| Cisco--Cisco Webex Meetings | A vulnerability in the integration of single sign-on (SSO) with Control Hub in Cisco Webex Services could have allowed an unauthenticated, remote attacker to impersonate any user within the service. This vulnerability existed because of improper certificate validation. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by connecting to a service endpoint and supplying a crafted token. A successful exploit could have allowed the attacker to gain unauthorized access to legitimate Cisco Webex services. | 2026-04-15 | 9.8 | CVE-2026-20184 |
| Cloud Foundry--UUA | Cloud Foundry UUA is vulnerable to a bypass that allows an attacker to obtain a token for any user and gain access to UAA-protected systems. This vulnerability exists when SAML 2.0 bearer assertions are enabled for a client, as the UAA accepts SAML 2.0 bearer assertions that are neither signed nor encrypted. This issue affects UUA from v77.30.0 to v78.7.0 (inclusive) and it affects CF Deployment from v48.7.0 to v54.14.0 (inclusive). | 2026-04-16 | 8.6 | CVE-2026-22734 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Dell--PowerProtect Data Domain BoostFS | Dell PowerProtect Data Domain BoostFS for client of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain an insufficiently protected credentials vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to credential exposure. The attacker may be able to use the exposed credentials to access the system with privileges of the compromised account. | 2026-04-17 | 7.8 | CVE-2025-36568 |
| easyappointments--Easy Appointments | The Easy Appointments plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.12.21 via the `/wp-json/wp/v2/eablocks/ea_appointments/` REST API endpoint. This is due to the endpoint being registered with `'permission_callback' => '__return_true'`, which allows access without any authentication or authorization checks. This makes it possible for unauthenticated attackers to extract sensitive customer appointment data including full names, email addresses, phone numbers, IP addresses, appointment descriptions, and pricing information. | 2026-04-17 | 7.5 | CVE-2026-2262 |
| Eaton--IPP software | Eaton Intelligent Power Protector (IPP) is affected by insecure library loading in its executable, which could lead to arbitrary code execution by an attacker with access to the software package. This security issue has been fixed in the latest version of Eaton IPP software which is available on the Eaton download center. | 2026-04-16 | 7.8 | CVE-2026-22619 |
| Eclipse Foundation--Eclipse Jetty | In Eclipse Jetty, the HTTP/1.1 parser is vulnerable to request smuggling when chunk extensions are used, similar to the "funky chunks" techniques outlined here: * https://w4ke.info/2025/06/18/funky-chunks.html * https://w4ke.info/2025/10/29/funky-chunks-2.html Jetty terminates chunk extension parsing at \r\n inside quoted strings instead of treating this as an error. POST / HTTP/1.1 Host: localhost Transfer-Encoding: chunked 1;ext="val X 0 GET /smuggled HTTP/1.1 ... Note how the chunk extension does not close the double quotes, and it is able to inject a smuggled request. | 2026-04-14 | 7.4 | CVE-2026-2332 |
| Festo--MSE6-C2M-5000-FB36-D-M-RG-BAR-M12L4-AGD | In products of the MSE6 product-family by Festo a remote authenticated, low privileged attacker could use functions of undocumented test mode which could lead to a complete loss of confidentiality, integrity and availability. | 2026-04-16 | 8.8 | CVE-2023-3634 |
| FirebirdSQL--firebird | Firebird is an open-source relational database management system. In versions FB3 of the client library placed incorrect data length values into XSQLDA fields when communicating with FB4 or higher servers, resulting in an information leak. This issue is fixed by upgrading to the FB4 client or higher. | 2026-04-17 | 7.9 | CVE-2025-65104 |
| Fortinet--FortiAnalyzer Cloud | A heap-based buffer overflow vulnerability in Fortinet FortiAnalyzer Cloud 7.6.2 through 7.6.4, FortiManager Cloud 7.6.2 through 7.6.4 may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests. Successful exploitation would require a large amount of effort in preparation because of ASLR and network segmentation | 2026-04-14 | 7.3 | CVE-2026-22828 |
| Grafana--Pyroscope | Pyroscope is an open-source continuous profiling database. The database supports various storage backends, including Tencent Cloud Object Storage (COS). If the database is configured to use Tencent COS as the storage backend, an attacker could extract the secret_key configuration value from the Pyroscope API. To exploit this vulnerability, an attacker needs direct access to the Pyroscope API. We highly recommend limiting the public internet exposure of all our databases, such that they are only accessible by trusted users or internal systems. This vulnerability is fixed in versions: 1.15.x: 1.15.2 and above. 1.16.x: 1.16.1 and above. 1.17.x: 1.17.0 and above (i.e. all versions). Thanks to Théo Cusnir for reporting this vulnerability to us via our bug bounty program. | 2026-04-15 | 9.1 | CVE-2025-41118 |
| Lenovo--Diagnostics | During an internal security assessment, a potential vulnerability was discovered in Lenovo Diagnostics and the HardwareScanAddin used in Lenovo Vantage that, during installation or when using hardware scan, could allow a local authenticated user to perform an arbitrary file write with elevated privileges. | 2026-04-15 | 7.1 | CVE-2026-0827 |
| livemesh--Livemesh Addons by Elementor | The Livemesh Addons for Elementor plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 9.0. This is due to insufficient sanitization of the template name parameter in the `lae_get_template_part()` function, which uses an inadequate `str_replace()` approach that can be bypassed using recursive directory traversal patterns. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the attacker to include and execute local files via the widget's template parameter granted they can trick an administrator into performing an action or install Elementor. | 2026-04-16 | 8.8 | CVE-2026-1620 |

# 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 Management Services allows an authorized attacker to elevate privileges locally. | 2026-04-14 | 7.8 | CVE-2026-20930 |
| n/a--Grocery Store Management System v1.0 | Improper input handling in /Grocery/search_products_itname.php, in anirudhkannan Grocery Store Management System 1.0, allows SQL injection via the sitem_name POST parameter. | 2026-04-14 | 9.8 | CVE-2025-63939 |
| n/a--manikandan580 School-management-system v1.0 | In manikandan580 School-management-system 1.0, a time-based blind SQL injection vulnerability exists in /studentms/admin/between-date-reprtsdetails.php through the fromdate POST parameter. | 2026-04-14 | 9.8 | CVE-2025-65135 |
| Nozomi Networks--Guardian | An access control vulnerability was discovered in the Threat Intelligence functionality due to a specific access restriction not being properly enforced for users with view-only privileges. An authenticated user with view-only privileges for the Threat Intelligence functionality can perform administrative actions on it, altering the rules configuration, and/or affecting their availability. | 2026-04-15 | 8.1 | CVE-2025-40897 |
| Nozomi Networks--Guardian | A Stored Cross-Site Scripting vulnerability was discovered in the Assets and Nodes functionality due to improper validation of an input parameter. An authenticated user with custom fields privileges can define a malicious custom field containing a JavaScript payload. When the victim views the Assets or Nodes pages, the XSS executes in their browser context, allowing the attacker to perform unauthorized actions as the victim, such as modify application data, disrupt application availability, and access limited sensitive information. | 2026-04-15 | 8.9 | CVE-2025-40899 |
| Owen--WebStack | The WebStack theme for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the io_img_upload() function in all versions up to, and including, 1.2024. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. | 2026-04-15 | 9.8 | CVE-2026-1555 |
| shahinurislam--Career Section | The Career Section plugin for WordPress is vulnerable to Cross-Site Request Forgery leading to Path Traversal and Arbitrary File Deletion in all versions up to, and including, 1.6. This is due to missing nonce validation and insufficient file path validation on the delete action in the 'appform_options_page_html' function. This makes it possible for unauthenticated attackers to delete arbitrary files on the server via a forged request, granted they can trick a site administrator into performing an action such as clicking on a link. | 2026-04-16 | 8.8 | CVE-2025-14868 |
| Splunk--Splunk Enterprise | In Splunk Enterprise versions below 10.2.1, 10.0.5, 9.4.10, and 9.3.11, and Splunk Cloud Platform versions below 10.4.2603.0, 10.3.2512.5, 10.2.2510.9, 10.1.2507.19, 10.0.2503.13, and 9.3.2411.127, a low-privileged user that does not hold the `admin` or `power` Splunk roles could potentially perform a Remote Code Execution (RCE) by uploading a malicious file to the `$SPLUNK_HOME/var/run/splunk/apptemp` directory due to improper handling and insufficient isolation of temporary files within the `apptemp` directory. | 2026-04-15 | 7.1 | CVE-2026-20204 |
| Splunk--Splunk MCP Server | In Splunk MCP Server app versions below 1.0.3 , a user who holds a role with access to the Splunk `_internal` index or possesses the high-privilege capability `mcp_tool_admin` could view users session and authorization tokens in clear text.<br><br>The vulnerability would require either local access to the log files or administrative access to internal indexes, which by default only the admin role receives. <br><br>Review roles and capabilities on your instance and restrict internal index access to administrator-level roles. See [Define roles on the Splunk platform with capabilities](https://docs.splunk.com/Documentation/Splunk/latest/Security/Rolesandcapabilities) and [Connecting to MCP Server and Admin settings](https://help.splunk.com/en/splunk-enterprise/mcp-server-for-splunk-platform/connecting-to-mcp-server-and-admin-settings) in the Splunk documentation for more information. | 2026-04-15 | 7.2 | CVE-2026-20205 |
| Ubiquiti Inc--UniFi Play PowerAmp | A malicious actor with access to the UniFi Play network could exploit a Path Traversal vulnerability found in the device firmware to write files on the system that could be used for a remote code execution (RCE). Affected Products: UniFi Play PowerAmp (Version 1.0.35 and earlier) UniFi Play Audio Port (Version 1.0.24 and earlier) Mitigation: Update UniFi Play PowerAmp to Version 1.0.38 or later Update UniFi Play Audio Port to Version 1.1.9 or later | 2026-04-13 | 9.8 | CVE-2026-22562 |
| Ubiquiti Inc--UniFi Play PowerAmp | A series of Improper Input Validation vulnerabilities could allow a Command Injection by a malicious actor with access to the UniFi Play network. Affected Products: UniFi Play PowerAmp (Version 1.0.35 and earlier) UniFi Play Audio | 2026-04-13 | 9.8 | CVE-2026-22563 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | Port (Version 1.0.24 and earlier) Mitigation: Update UniFi Play PowerAmp to Version 1.0.38 or later Update UniFi Play Audio Port to Version 1.1.9 or later | | | |
| Ubiquiti Inc--UniFi Play PowerAmp | An Improper Access Control vulnerability could allow a malicious actor with access to the UniFi Play network to enable SSH to make unauthorized changes to the system. Affected Products: UniFi Play PowerAmp (Version 1.0.35 and earlier) UniFi Play Audio Port (Version 1.0.24 and earlier) Mitigation: Update UniFi Play PowerAmp to Version 1.0.38 or later Update UniFi Play Audio Port to Version 1.1.9 or later | 2026-04-13 | 9.8 | CVE-2026-22564 |
| Ubiquiti Inc--UniFi Play PowerAmp | An Improper Access Control vulnerability could allow a malicious actor with access to the UniFi Play network to obtain UniFi Play WiFi credentials. Affected Products: UniFi Play PowerAmp (Version 1.0.35 and earlier) UniFi Play Audio Port (Version 1.0.24 and earlier) Mitigation: Update UniFi Play PowerAmp to Version 1.0.38 or later Update UniFi Play Audio Port to Version 1.1.9 or later | 2026-04-13 | 7.5 | CVE-2026-22566 |
| WC Lovers--WCFM Marketplace | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WC Lovers WCFM Marketplace allows SQL Injection.This issue affects WCFM Marketplace: from n/a through 3.7.1. | 2026-04-15 | 7.6 | CVE-2025-63029 |
| WSO2--WSO2 API Manager | The XML parsers within multiple WSO2 products accept user-supplied XML data without properly configuring to prevent the resolution of external entities. This omission allows malicious actors to craft XML payloads that exploit the parser's behavior, leading to the inclusion of external resources. By leveraging this vulnerability, an attacker can read confidential files from the file system and access limited HTTP resources reachable by the product. Additionally, the vulnerability can be exploited to perform denial of service attacks by exhausting server resources through recursive entity expansion or fetching large external resources. | 2026-04-16 | 7.5 | CVE-2024-2374 |
| Cewe-Photoworld--CEWE Photoshow | CEWE Photoshow 6.3.4 contains a buffer overflow vulnerability in the login dialog that allows attackers to crash the application by submitting oversized input. Attackers can inject 4000 bytes of data into the email address and password fields to trigger a denial of service condition. | 2026-04-26 | 7.5 | CVE-2018-25294 |
| Elba--ELBA5 | ELBA5 5.8.0 contains a remote code execution vulnerability that allows attackers to obtain database credentials and execute arbitrary commands with SYSTEM level permissions. Attackers can connect to the database using default connector credentials, decrypt the DBA password, and execute commands via the xp_cmdshell stored procedure or add backdoor users to the BEDIENER table. | 2026-04-22 | 9.8 | CVE-2018-25272 |
| faleemi--Faleemi Desktop Software | Faleemi Desktop Software 1.8.2 contains a local buffer overflow vulnerability in the Device alias field that allows local attackers to trigger a structured exception handler (SEH) overwrite. Attackers can craft a malicious payload and paste it into the Device alias field within the Managing Log interface to execute arbitrary code with calculator proof-of-concept execution. | 2026-04-26 | 8.4 | CVE-2018-25263 |
| Fortra--GoAnywhere MFT | The login limit is not enforced on the SFTP service of Fortra's GoAnywhere MFT prior to 7.10.0 if the Web User attempting to be logged in to is configured to log in with an SSH Key, making the SSH key vulnerable to being guessed via Brute Force. | 2026-04-21 | 7.3 | CVE-2025-14362 |
| Iperiusbackup--Iperius Backup | Iperius Backup 5.8.1 contains a local buffer overflow vulnerability in the structured exception handling (SEH) mechanism that allows local attackers to execute arbitrary code by supplying a malicious file path. Attackers can create a backup job with a crafted payload in the external file location field that triggers a buffer overflow when the backup job executes, enabling code execution with application privileges. | 2026-04-22 | 8.4 | CVE-2018-25261 |
| Lizardsystems--LanSpy | LanSpy 2.0.1.159 contains a local buffer overflow vulnerability in the scan section that allows local attackers to execute arbitrary code by exploiting structured exception handling mechanisms. Attackers can craft malicious payloads using egghunter techniques to locate and execute shellcode, triggering code execution through SEH chain manipulation and controlled jumps. | 2026-04-22 | 8.4 | CVE-2018-25265 |
| Lizardsystems--LanSpy | LanSpy 2.0.1.159 contains a local buffer overflow vulnerability that allows attackers to overwrite the instruction pointer by supplying oversized input to the scan field. Attackers can craft a payload with 688 bytes of padding followed by 4 bytes of controlled data to crash the application or potentially achieve code execution. | 2026-04-22 | 8.4 | CVE-2018-25268 |
| Lizardsystems--Terminal Services Manager | Terminal Services Manager 3.1 contains a stack-based buffer overflow vulnerability in the computer names field that allows local attackers to execute arbitrary code by triggering structured exception handling. Attackers can craft a malicious input file with shellcode and jump instructions that overwrite the SEH handler pointer to execute calc.exe or other payloads when imported through the add computers wizard. | 2026-04-22 | 8.4 | CVE-2018-25259 |
| Magix--MAGIX Music Editor | MAGIX Music Editor 3.1 contains a buffer overflow vulnerability in the FreeDB Proxy Options dialog that allows local attackers to execute arbitrary code by | 2026-04-22 | 8.4 | CVE-2018-25260 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | exploiting structured exception handling. Attackers can craft a malicious payload, paste it into the Server field via the CD menu's FreeDB Proxy Options, and trigger code execution when settings are accepted. | | | |
| Securimport--iSmartViewPro | iSmartViewPro 1.5 contains a structured exception handling (SEH) buffer overflow vulnerability in the 'Save Path for Snapshot and Record file' field that allows local attackers to execute arbitrary code. Attackers can input a crafted payload exceeding 260 bytes through the System Setup interface to overwrite SEH records and execute shellcode with application privileges. | 2026-04-26 | 8.4 | CVE-2018-25283 |
| Thinkphp--ThinkPHP | ThinkPHP 5.0.23 contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary PHP code by invoking functions through the routing parameter. Attackers can craft requests to the index.php endpoint with malicious function parameters to execute system commands with application privileges. | 2026-04-22 | 9.8 | CVE-2018-25270 |
| Acrel Electrical--ECEMS Enterprise Microgrid Energy Efficiency Management System | A flaw has been found in Acrel Electrical ECEMS Enterprise Microgrid Energy Efficiency Management System 1.3.0. The impacted element is an unknown function of the file /SubstationWEBV2/main/elecMaxMinAvgValue. Executing a manipulation of the argument fCircuitids can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 7.3 | CVE-2026-7694 |
| Acrel Electrical--EEMS Enterprise Power Operation and Maintenance Cloud Platform | A vulnerability has been found in Acrel Electrical EEMS Enterprise Power Operation and Maintenance Cloud Platform 1.3.0. This affects an unknown function of the file /SubstationWEBV2/main/elecMaxMinAvgValue. The manipulation of the argument fCircuitids leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 7.3 | CVE-2026-7695 |
| Alloksoft--Allok AVI to DVD SVCD VCD Converter | Allok AVI to DVD SVCD VCD Converter 4.0.1217 contains a structured exception handling (SEH) based buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious string in the License Name field. Attackers can craft a payload with junk data, NSEH bypass, SEH handler address, and shellcode that triggers the overflow when pasted into the License Name field and the Register button is clicked, resulting in code execution. | 2026-04-29 | 7.8 | CVE-2018-25302 |
| Alloksoft--Allok Video to DVD Burner | Allok Video to DVD Burner 2.6.1217 contains a stack-based buffer overflow vulnerability in the License Name field that allows local attackers to execute arbitrary code by triggering a structured exception handler (SEH) overwrite. Attackers can craft a malicious input string with 780 bytes of junk data followed by SEH chain pointers and shellcode, then paste it into the License Name field during registration to achieve code execution. | 2026-04-29 | 8.4 | CVE-2018-25303 |
| Alloksoft--Video Joiner | Alloksoft Video joiner 4.6.1217 contains a buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious string in the License Name field. Attackers can craft a payload with structured exception handler (SEH) overwrite and shellcode to achieve code execution when the application processes the license registration input. | 2026-04-29 | 8.4 | CVE-2018-25315 |
| Alloksoft--WMV to AVI MPEG DVD WMV Converter | Allok soft WMV to AVI MPEG DVD WMV Converter 4.6.1217 contains a buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying an oversized string in the License Name field. Attackers can craft a malicious input containing shellcode with structured exception handler (SEH) overwrite to bypass protections and execute code with application privileges. | 2026-04-29 | 8.4 | CVE-2018-25314 |
| AV Stumpfl--Pixera Two Media Server | A flaw has been found in AV Stumpfl Pixera Two Media Server up to 25.2 R2. Impacted is an unknown function of the component Websocket API. This manipulation causes code injection. The attack can be initiated remotely. The exploit has been published and may be used. Upgrading to version 25.2 R3 is recommended to address this issue. Upgrading the affected component is advised. | 2026-05-03 | 7.3 | CVE-2026-7703 |
| benjaminprojas--WP Editor | The WP Editor plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.9.2. This is due to missing nonce verification in the 'add_plugins_page' and 'add_themes_page' functions. This makes it possible for unauthenticated attackers to overwrite arbitrary plugin and theme PHP files with attacker-controlled code via a forged request, granted they can trick a site administrator into performing an action such as clicking a link. | 2026-05-01 | 8.8 | CVE-2026-3772 |
| carazo--Import and export users and customers | The Import and export users and customers plugin for WordPress is vulnerable to Privilege Escalation in all versions up to and including 2.0.8 via the `save_extra_user_profile_fields()` function. This is due to an incomplete blocklist that correctly restricts capability meta keys for the primary site (e.g., `wp_capabilities`, `wp_user_level`) but fails to block the equivalent meta keys for any other subsite in a WordPress Multisite network (e.g., `wp_2_capabilities`, `wp_2_user_level`), allowing these keys to pass the `in_array()` check and be | 2026-05-02 | 8.8 | CVE-2026-7641 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | written directly to user meta via `update_user_meta()`. This makes it possible for authenticated attackers, with Subscriber-level access and above, to escalate their privileges to Administrator on any subsite within the Multisite network by submitting a crafted profile update to `/wp-admin/profile.php`. Exploitation requires that an administrator has previously imported a CSV file containing multisite-prefixed capability column headers and has enabled the 'Show fields in profile?' option, which causes those keys to be stored in the `acui_columns` option and exposed as editable fields on the user profile page. | | | |
| Carlson Software--VASCO-B GNSS Receiver | The Carlson VASCO-B GNSS Receiver lacks an authentication mechanism, allowing an attacker with network access to directly access and modify its configuration and operational functions without needing credentials. | 2026-04-28 | 9.4 | CVE-2026-3893 |
| chartbrew--chartbrew | Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. In version 4.9.0, Chartbrew allows authenticated users with access to one project to update or delete a SharePolicy record that belongs to a different project. The affected routes authorize the caller against the project in the URL path, but they never verify that policy_id belongs to that project. This permits cross-project modification of dashboard sharing rules, including visibility, password requirements, allowed parameters, and expiration settings. This issue has been patched in version 5.0.0. | 2026-04-30 | 8.1 | CVE-2026-40600 |
| chartbrew--chartbrew | Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. In version 4.9.0, Chartbrew exposes public chart retrieval and export routes that only verify project-level public access and, for exports, a team-level export toggle. The routes do not verify whether the target chart is actually allowed on the public report or whether the governing SharePolicy permits public access. An unauthenticated attacker who knows a chart identifier in a public project can read or export chart data for charts that were intentionally hidden from the report. This issue has been patched in version 5.0.0. | 2026-04-30 | 7.5 | CVE-2026-40595 |
| chartbrew--chartbrew | Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. In version 4.9.0, Chartbrew exposes POST /api/chart/:chart_id/query without authentication. The endpoint only checks team.allowReportRefresh and does not verify that the target chart belongs to a public report, that the project is public, or that sharing policy allows the operation. An unauthenticated attacker who knows a chart identifier can trigger a data refresh and retrieve the current data of private charts. This issue has been patched in version 5.0.0. | 2026-04-30 | 7.5 | CVE-2026-40601 |
| ChatGPTNextWeb--NextChat | A vulnerability has been found in ChatGPTNextWeb NextChat up to 2.16.1. Affected is the function addMcpServer of the file app/mcp/actions.ts. The manipulation leads to improper 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. | 2026-05-02 | 7.3 | CVE-2026-7644 |
| Cockpit--Cockpit CMS | Cockpit CMS contains an authenticated remote code execution vulnerability in the /cockpit/collections/save_collection endpoint that allows authenticated attackers with collection management privileges to inject arbitrary PHP code into collection rules parameters. Attackers can inject malicious PHP code through rule parameters which is written directly to server-side PHP files and executed via include() to achieve arbitrary command execution on the underlying server. | 2026-04-29 | 8.8 | CVE-2026-34965 |
| code-projects--Online Hospital Management System | A vulnerability was determined in code-projects Online Hospital Management System 1.0. This affects an unknown function of the file /viewappointment.php. This manipulation of the argument delid causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. | 2026-05-02 | 7.3 | CVE-2026-7632 |
| Cozmoslabs--Profile Builder Pro | The Profile Builder Pro plugin for WordPress is vulnerable to PHP Object Injection in all versions up to and including 3.14.5. This is due to the use of PHP's maybe_unserialize() function on the attacker-controlled 'args' POST parameter within the wppb_request_users_pins_action_callback() AJAX handler, which lacked any nonce verification, type checking, or input validation before deserialization. Because the handler was registered with both wp_ajax_ and wp_ajax_nopriv_ hooks, it was reachable by completely unauthenticated users. This makes it possible for unauthenticated attackers to inject arbitrary PHP objects into application memory. | 2026-05-02 | 8.1 | CVE-2026-7647 |
| CryptPad--CryptPad | CryptPad 2025.3.1 allows unbounded WebSocket frame flood. A remote, unauthenticated attacker can significantly degrade or deny service for all users of a CryptPad instance. Fixed in 2026.2.2. | 2026-04-30 | 7.5 | CVE-2025-51846 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| cyberhobo--Geo Mashup | The Geo Mashup plugin for WordPress is vulnerable to Time-Based SQL Injection via the 'sort' parameter in all versions up to, and including, 1.13.18. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. The `esc_sql()` function is applied but is ineffective in the `ORDER BY` context because the value is not enclosed in quotes. Additionally, while a `sanitize_sort_arg()` allowlist-based sanitizer was added in version 1.13.18, it is only applied in the AJAX code path (`sanitize_query_args()`) and not in the `render-map.php` or template tag code paths. 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 via a time-based blind approach. | 2026-05-02 | 7.5 | CVE-2026-4060 |
| cyberhobo--Geo Mashup | The Geo Mashup plugin for WordPress is vulnerable to Time-Based SQL Injection via the 'map_post_type' parameter in all versions up to, and including, 1.13.18. This is due to the `SearchResults` hook explicitly calling `stripslashes_deep($_POST)` which removes WordPress magic quotes protection, followed by the unsanitized `map_post_type` value being concatenated into an `IN(...)` clause without `esc_sql()` or `$wpdb->prepare()`. The 'any' branch of the same code correctly applies `array_map('esc_sql', ...)`, but the else branch does not. 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 via a time-based blind approach. Exploitation requires the Geo Search feature to be enabled in plugin settings. | 2026-05-02 | 7.5 | CVE-2026-4061 |
| cyberhobo--Geo Mashup | The Geo Mashup plugin for WordPress is vulnerable to Time-Based SQL Injection via the 'object_ids' and 'exclude_object_ids' parameters in all versions up to, and including, 1.13.18. This is due to insufficient escaping on the user supplied parameters and lack of sufficient preparation on the existing SQL query. The `esc_sql()` function is applied but is ineffective because the values are placed in an unquoted `IN(...)` / `NOT IN(...)` SQL context - `esc_sql()` only escapes quote characters and provides no protection against parenthesis or SQL keyword injection. Additionally, while a numeric-only sanitizer exists in `sanitize_query_args()`, it is only applied in the AJAX code path and not in the `render-map.php` or template tag code paths. 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 via a time-based blind approach. | 2026-05-02 | 7.5 | CVE-2026-4062 |
| Dell--iDRAC10 | Dell iDRAC10, versions 1.20.70.50 and 1.30.05.10, contains an Insufficiently Protected Credentials vulnerability. A race condition vulnerability exists that could allow an authenticated low-privileged attacker to gain elevated access. | 2026-04-29 | 7.1 | CVE-2026-35155 |
| Directorist Booking--Directorist Booking | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Directorist Booking allows SQL Injection.This issue affects Directorist Booking: from n/a before 3.0.2. | 2026-04-27 | 9.3 | CVE-2026-22336 |
| Directorist--Directorist Social Login | Incorrect Privilege Assignment vulnerability in Directorist Directorist Social Login allows Privilege Escalation.This issue affects Directorist Social Login: from n/a before 2.1.4. | 2026-04-27 | 9.8 | CVE-2026-22337 |
| donmik--Buddypress Xprofile Custom Fields Type | BuddyPress Xprofile Custom Fields Type 2.6.3 contains a remote code execution vulnerability that allows authenticated users to delete arbitrary files by manipulating unescaped POST parameters. Attackers can modify the field_hiddenfile and field_deleteimg parameters during profile editing to unlink files from the server. | 2026-04-29 | 8.8 | CVE-2018-25308 |
| Easy MPEG--Easy MPEG to DVD Burner | Easy MPEG to DVD Burner 1.7.11 contains a structured exception handling (SEH) local buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious username string. Attackers can craft a payload containing junk data, SEH chain pointers, and shellcode that overwrites the SEH handler to redirect execution and run arbitrary commands like opening calc.exe. | 2026-04-29 | 8.4 | CVE-2018-25301 |
| Edimax--BR-6208AC | A vulnerability was detected in Edimax BR-6208AC up to 1.02. Affected is an unknown function of the file /goform/setWAN. Performing a manipulation of the argument pptpDfGateway results in buffer overflow. The attack may be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 8.8 | CVE-2026-7685 |
| Edimax--BR-6428nC | A security vulnerability has been detected in Edimax BR-6428nC up to 1.16. This impacts an unknown function of the file /goform/setWAN. Such manipulation of the argument pptpDfGateway leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 8.8 | CVE-2026-7684 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Filehippo--Free Download Manager | Free Download Manager 2.0 Built 417 contains a local buffer overflow vulnerability in the URL import functionality that allows attackers to trigger a structured exception handler (SEH) chain exploitation. Attackers can craft a malicious URL file that, when imported through the File > Import > Import lists of downloads menu, causes a buffer overflow in the Location header response that overwrites the SEH chain and executes arbitrary code. | 2026-04-29 | 8.4 | CVE-2018-25304 |
| innocommerce--InnoShop | A vulnerability has been found in innocommerce InnoShop up to 0.7.8. The affected element is the function InstallServiceProvider::boot of the file innopacks/install/src/InstallServiceProvider.php of the component Installation Endpoint. The manipulation leads to improper authentication. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The identifier of the patch is 45758e4ec22451ab944ae2ae826b1e70f6450dc9. It is recommended to apply a patch to fix this issue. | 2026-05-02 | 7.3 | CVE-2026-7630 |
| 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/UserSel.aspx. This manipulation of the argument DeptIDList causes sql injection. The attack is possible to be carried out 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. | 2026-05-02 | 7.3 | CVE-2026-7670 |
| marketingfire--Widget Options Advanced Conditional Visibility for Gutenberg Blocks & Classic Widgets | The Widget Options - Advanced Conditional Visibility for Gutenberg Blocks & Classic Widgets plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.2.2 via the Display Logic feature. This is due to the plugin using eval() on user-supplied Display Logic expressions with an insufficient blocklist/allowlist that can be bypassed using array_map with string concatenation, combined with a lack of authorization enforcement on the extended_widget_opts_block attribute. This makes it possible for authenticated attackers, with Contributor-level access and above, to execute code on the server. The vulnerability was partially patched in version 4.2.0. | 2026-05-02 | 8.8 | CVE-2026-2052 |
| Mersenne--Prime95 | Prime95 29.4b8 contains a local buffer overflow vulnerability that allows attackers to execute arbitrary code by exploiting structured exception handling (SEH) mechanisms. Attackers can inject malicious payload through the optional proxy hostname field in the PrimeNet connection settings to trigger the overflow and execute system commands. | 2026-04-29 | 8.4 | CVE-2018-25299 |
| MikroTik--RouterOS | A vulnerability was identified in MikroTik RouterOS 6.49.8. This vulnerability affects the function ASN1_STRING_data in the library nova/lib/www/scep.p of the component SCEP Endpoint. The manipulation of the argument transactionID/messageType leads to out-of-bounds read. The attack may be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-02 | 7.3 | CVE-2026-7668 |
| Milesight--MS-Cxx63-PD | Specific firmware versions of Milesight AIOT cameras use SSL certificates with default private keys. | 2026-04-27 | 9.8 | CVE-2026-32644 |
| Milesight--MS-Cxx63-PD | An out-of-bounds memory access vulnerability exists in specific firmware versions of Milesight AIOT cameras. | 2026-04-27 | 8.8 | CVE-2026-20766 |
| Milesight--MS-Cxx63-PD | Specific firmware versions of Milesight AIOT camera firmware contain hard-coded credentials. | 2026-04-27 | 8.8 | CVE-2026-27785 |
| mybb--MyBB Recent threads | MyBB Recent threads 17.0 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts by creating threads with crafted subject lines. Attackers can create threads with script tags in the subject parameter to execute arbitrary JavaScript in the browsers of all users viewing the index page. | 2026-04-29 | 7.2 | CVE-2018-25309 |
| n/a-- cannelloni v2.0.0 | Buffer overflow vulnerability in cannelloni v2.0.0 in CAN frame parsing in parser.cpp in function parseCANFrame, and decoder.cpp in function decodeFrame allowing remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via crafted CAN FD frames. | 2026-05-01 | 9.8 | CVE-2026-37539 |
| n/a-- OVMS3 3.3.005 | Buffer overflow vulnerability in Open Vehicle Monitoring System 3 (OVMS3) 3.3.005. In canformat_gvret.cpp, the length field in GVRET binary data is not properly validated, allowing remote attackers to cause a denial of service or possibly execute arbitrary code via crafted GVRET frames. | 2026-05-01 | 10 | CVE-2026-37541 |
| n/a-- Vanetza V2X v26.02 | An issue was discovered in Vanetza V2X v26.02 allowing remote unauthorized attackers to cause a denial of service. The vulnerability exists in the GeoNetworking packet processing pipeline where OpenSSL exceptions from ECC point validation (invalid compressed point, point not on curve) are not properly caught by the Router::indicate() call chain. The openssl_wrapper.cpp check() function (line 19) throws openssl::Exception when OpenSSL operations fail. The parser's catch block in parse_secured() should catch these, but the exception escapes through | 2026-05-01 | 7.5 | CVE-2026-37554 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | subsequent processing stages (indicate_common, indicate_extended). This causes std::terminate, crashing the V2X receiver. | | | |
| n/a--(UDS) & OBD-II (On Board Diagnostics for Vehicles) | miaofng/uds-c commit e506334e270d77b20c0bc259ac6c7d8c9b702b7a (2016-10-05) contains a stack buffer overflow in send_diagnostic_request. A 6-byte stack buffer (MAX_DIAGNOSTIC_PAYLOAD_SIZE=6) receives memcpy at offset 1+pid_length with payload_length bytes. MAX_UDS_REQUEST_PAYLOAD_LENGTH=7, so 1+2+7=10 exceeds buffer by 4 bytes. No bounds check on payload_length before memcpy. | 2026-05-01 | 8.8 | CVE-2026-37536 |
| n/a--Automotive Grade Linux (AGL) | AGL app-framework-main thru 17.1.12 contains a Zip Slip path traversal vulnerability (CWE-22) combined with a TOCTOU race condition (CWE-367) in the widget installation flow. The is_valid_filename function in wgtpkg-zip.c validates ZIP entry names but does not check for dot notation directory traversal sequences it only blocks absolute paths. The zread extraction function uses openat(workdirfd, filename, O_CREAT) which resolves dot notation values relative to the work directory, allowing files to be written anywhere on the filesystem. Critically, in function install_widget in file wgtpkg-install.c, extraction via zread occurs BEFORE signature verification via check_all_signatures. Even if signature verification fails, the error cleanup (remove_workdir) only deletes the temporary work directory files written outside via path traversal persist permanently. | 2026-05-01 | 9.8 | CVE-2026-37531 |
| n/a--Automotive Grade Linux (AGL) afb-daemon v19.90.0 | AGL app-framework-binder (afb-daemon) through v19.90.0 contains a privilege escalation vulnerability in the supervision Do command. The on_supervision_call function in src/afb-supervision.c explicitly nullifies the request credentials by calling afb_context_change_cred(&xreq->context, NULL) before dispatching an attacker-controlled API call via xapi->itf->call(xapi->closure, xreq). The NULL propagation chain through afb-context.c:110 (context->credentials = afb_cred_addref(NULL)) and afb-cred.c:163 (returns NULL when cred is NULL) confirms that credentials are zeroed before the target API executes. The attacker controls both api and verb parameters via JSON input, allowing execution of any registered API with a NULL credential context. APIs that rely on context->credentials for authorization decisions may fail open when receiving NULL credentials, enabling privilege escalation. This vulnerability was introduced in commit abbb4599f0b921c6f434b6bd02bcfb277eecf745 on 2018-02-14. | 2026-05-01 | 7.8 | CVE-2026-37525 |
| n/a--Automotive Grade Linux (AGL) afb-daemon v19.90.0 | AGL app-framework-binder (afb-daemon) through v19.90.0 allows any local process to execute privileged supervision commands (Exit, Do, Sclose, Config, Trace, Debug, Token, slist) without authentication via the abstract Unix socket @urn:AGL:afs:supervision:socket. The on_supervision_call function in src/afb-supervision.c dispatches all 8 commands without any credential verification. The abstract socket has no DAC protection, as acknowledged in the official CAUTION comment in src/afs-supervision.h. This allows a low-privileged local process to kill the daemon (DoS via Exit command), execute arbitrary API calls (via Do command), close arbitrary user sessions (via Sclose command), or leak the entire global configuration (via Config command). The vulnerability was introduced in commit b8c9d5de384efcfa53ebdb3f0053d7b3723777e1 on 2017-06-29. | 2026-05-01 | 7.8 | CVE-2026-37526 |
| n/a--Automotive Grade Linux (AGL) aglservice v17.1.12 | AGL agl-service-can-low-level thru 17.1.12 contains a heap buffer over-read in the isotp-c library. In isotp_continue_receive (receive.c:87-89), the payload_length for a Single Frame is extracted from a 4-bit nibble in the CAN frame data, yielding values 0-15. However, a standard CAN frame is only 8 bytes, with payload starting at data[1] (7 bytes available). When payload_length exceeds the available data (e.g., nibble=15 but only 7 payload bytes exist), memcpy(message.payload, &data[1], payload_length) reads up to 8 bytes past the end of the data buffer. | 2026-05-01 | 7.1 | CVE-2026-37532 |
| n/a--Automotive Grade Linux (AGL) isotp-c | openxc/isotp-c thru commit 5a5d19245f65189202719321facd49ce6f5d46ac (2021-08-09) contains an out-of-bounds read in the ISO-TP Single Frame receive handler, where the 4-bit payload length nibble is used directly as the memcpy size without validating it against the actual CAN data length. A malicious CAN frame with an oversized length nibble can cause memory reads beyond the buffer, allowing attackers to cause a denial of service, or gain sensitive information. | 2026-05-01 | 7.1 | CVE-2026-37535 |
| n/a--django-mdeditor | All versions of the package django-mdeditor are vulnerable to Missing Authentication for Critical Function in the image upload endpoint. An attacker can upload malicious files and achieve arbitrary code execution since this endpoint lacks authentication protection and proper sanitisation of file names. | 2026-04-30 | 7.1 | CVE-2025-13030 |
| n/a--libssh2 | A security vulnerability has been detected in libssh2 up to 1.11.1. The impacted element is the function userauth_password of the file src/userauth.c. Such manipulation of the argument username_len/password_len leads to integer overflow. The attack may be launched remotely. The name of the patch is | 2026-05-01 | 7.3 | CVE-2026-7598 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | 256d04b60d80bf1190e96b0ad1e91b2174d744b1. A patch should be applied to remediate this issue. | | | |
| n/a--MindsDB | A weakness has been identified in MindsDB up to 26.01. This impacts the function exec of the file mindsdb/integrations/handlers/byom_handler/proc_wrapper.py of the component Engine Handler. Executing a manipulation 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. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 7.3 | CVE-2026-7711 |
| n/a--MixPHP Framework 2.x | Unsafe deserialization vulnerability in MixPHP Framework 2.x thru 2.2.17. The sync-invoke TCP server (Server.php:87) receives data from a TCP socket, passes it directly to Opis\Closure\unserialize(), then executes the result via call_user_func(). No authentication or signature verification exists on the TCP connection. An attacker with access to the localhost TCP port (server binds 127.0.0.1) can send a crafted serialized PHP closure to achieve arbitrary code execution. | 2026-05-01 | 8.4 | CVE-2026-37552 |
| n/a--Open-SAE-J1939 (Daniel Martensson) | collin80/Open-SAE-J1939 thru commit 744024d4306bc387857dfce439558336806acb06 (2023-03-08) contains an integer underflow leading to out-of-bounds write in Transport Protocol Data Transfer handling. At line 23: uint8_t index = data[0] - 1. When data[0] (sequence number from CAN frame) is 0, index underflows to 255. Subsequent write at tp_dt->data[255*7 + i-1] reaches offset 1791, exceeding the MAX_TP_DT buffer (1785 bytes) by 6 bytes. | 2026-05-01 | 8.1 | CVE-2026-37537 |
| openampproject[.]org--OpenAMP v2025.10.0 | OpenAMP v2025.10.0 ELF loader contains an integer overflow vulnerability in firmware image parsing. In elf_loader.c, it performs multiplication of two attacker-controlled 16-bit values from the ELF header without overflow checking. On 32-bit embedded systems (STM32MP1, Zynq, i.MX), large values can cause the product to wrap around to a small value. | 2026-05-01 | 8.4 | CVE-2026-37540 |
| opencats--OpenCATS | OpenCATS prior to commit 3002a29 contains a PHP code injection vulnerability in the installer AJAX endpoint that allows unauthenticated attackers to execute arbitrary code by injecting PHP statements into the databaseConnectivity action parameter. Attackers can break out of the define() string context in config.php using a single quote and statement separator to inject malicious PHP code that persists and executes on every subsequent page load when the installation wizard remains incomplete. | 2026-04-28 | 8.1 | CVE-2026-27760 |
| OPPO--ColorOS Assistant | ColorOS Assistant has an unauthenticated start-download channel, leading to file path traversal. | 2026-04-30 | 7.1 | CVE-2026-22070 |
| redhat[.]com--DTLS | A flaw in GnuTLS DTLS handshake parsing allows malformed fragments with zero length and non-zero offset, leading to an integer underflow during reassembly and resulting in an out-of-bounds read. This issue is remotely exploitable and may cause information disclosure or denial of service. | 2026-04-30 | 7.5 | CVE-2026-33845 |
| reputeinfosystems--ARMember Membership Plugin, Content Restriction, Member Levels, User Profile & User signup | The ARMember - Membership Plugin, Content Restriction, Member Levels, User Profile & User signup plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'orderby' parameter in all versions up to, and including, 4.0.60 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. | 2026-05-02 | 7.5 | CVE-2026-7649 |
| Shenzhen Libituo Technology--LBT-T300-HW1 | A flaw has been found in Shenzhen Libituo Technology LBT-T300-HW1 up to 1.2.8. This issue affects the function start_single_service of the component Web Management Interface. Executing a manipulation of the argument vpn_pptp_server/vpn_l2tp_server can lead to buffer overflow. The attack can be executed remotely. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 8.8 | CVE-2026-7674 |
| Shenzhen Libituo Technology--LBT-T300-HW1 | A vulnerability has been found in Shenzhen Libituo Technology LBT-T300-HW1 up to 1.2.8. Impacted is the function start_lan of the file /apply.cgi. The manipulation of the argument Channel/ApCliSsid leads to buffer overflow. 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. | 2026-05-03 | 8.8 | CVE-2026-7675 |
| synway[.]net--SMG Gateway Management | Synway SMG Gateway Management Software contains an OS command injection vulnerability in the RADIUS configuration endpoint at /en/9-2radius.php where the radius_address POST parameter is split and interpolated directly into a sed command without sanitization. An unauthenticated remote attacker can inject arbitrary shell commands by submitting a POST request with crafted radius_address, radius_address2, shared_secret2, source_ip, timeout, or retry | 2026-04-30 | 9.8 | CVE-2025-71284 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | parameters along with save=1 and enable_radius=1 to achieve remote code execution. Exploitation evidence was first observed by the Shadowserver Foundation on 2025-07-11 (UTC). | | | |
| Sysgauge--SysGauge Pro | SysGauge Pro 4.6.12 contains a local buffer overflow vulnerability in the Register function that allows local attackers to overwrite the structured exception handler by supplying a crafted unlock key. Attackers can inject shellcode through the Unlock Key field during registration to execute arbitrary code with application privileges. | 2026-04-29 | 8.4 | CVE-2018-25307 |
| tendacn[.]com--W308R | Tenda W308R v2 V5.07.48 contains a cookie session weakness vulnerability that allows unauthenticated attackers to modify DNS settings by exploiting insufficient session validation. Attackers can send GET requests to the goform/AdvSetDns endpoint with a crafted admin language cookie to change DNS servers and redirect user traffic to malicious sites. | 2026-04-29 | 9.8 | CVE-2018-25316 |
| tendacn[.]com--FH303/A300 | Tenda FH303/A300 firmware V5.07.68_EN contains a session weakness vulnerability that allows unauthenticated attackers to modify DNS settings by exploiting insufficient cookie validation. Attackers can send GET requests to the /goform/AdvSetDns endpoint with a crafted admin cookie to change DNS servers and redirect user traffic to malicious sites. | 2026-04-29 | 9.8 | CVE-2018-25318 |
| tendacn[.]com--W3002R | Tenda W3002R/A302/W309R wireless routers version V5.07.64_en contain a cookie session weakness vulnerability that allows unauthenticated attackers to modify DNS settings by exploiting insufficient session validation. Attackers can send GET requests to the /goform/AdvSetDns endpoint with a crafted admin language cookie to change primary and secondary DNS servers, redirecting user traffic to malicious DNS servers. | 2026-04-29 | 9.8 | CVE-2018-25317 |
| Tiandy--Easy7 Integrated Management Platform | A vulnerability was identified in Tiandy Easy7 Integrated Management Platform 7.17.0. Affected by this vulnerability is an unknown functionality of the file /Easy7/rest/systemInfo/updateDbBackupInfo. Such manipulation of the argument week leads to os command injection. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 7.3 | CVE-2026-7698 |
| TRENDnet--TEW-821DAP | A security vulnerability has been detected in TRENDnet TEW-821DAP 1.12B01. Impacted is the function auto_update_firmware of the component Firmware Udpate. The manipulation of the argument str leads to buffer overflow. The attack may be initiated remotely. The vendor explains: "That firmware version will only work on our hardware version v1.xR. We have already EOL that product 8 years ago and are no longer selling". This vulnerability only affects products that are no longer supported by the maintainer. | 2026-05-02 | 8.8 | CVE-2026-7607 |
| VEGA Grieshaber--VEGAPULS 6X Two-wire PROFINET, Modbus TCP, OPC UA (Ethernet-APL) | An unsecured configuration interface on affected devices allows unauthenticated remote attackers to access sensitive information, including hashed credentials and access codes. | 2026-04-28 | 7.5 | CVE-2026-3323 |
| wclovers--WCFM Frontend Manager for WooCommerce | The WCFM - Frontend Manager for WooCommerce along with Bookings Subscription Listings Compatible plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 6.7.25 via the 'wcfm_delete_wcfm_customer' due to missing validation on the 'customerid' user controlled key. This makes it possible for authenticated attackers, with Vendor-level access and above, to delete arbitrary users, including Administrators. | 2026-05-02 | 8.1 | CVE-2026-2554 |
| Weaver Network Co., Ltd.--E-cology | Weaver (Fanwei) E-cology 9.5 versions prior to 10.52 contain an arbitrary file read vulnerability in the XmlRpcServlet interface at the XML-RPC endpoint that allows unauthenticated remote attackers to read arbitrary files by supplying file paths to the WorkflowService.getAttachment and WorkflowService.LoadTemplateProp methods. Attackers can exploit these methods without authentication to retrieve sensitive files including system configuration files and database credentials from the server. Exploitation evidence was first observed by the Shadowserver Foundation on 2022-12-14 (UTC). | 2026-04-30 | 7.5 | CVE-2022-50992 |
| Weaver Network Co., Ltd.--E-office | Weaver (Fanwei) E-office versions prior to 10.0_20221201 contain an unauthenticated arbitrary file upload vulnerability in the OfficeServer.php endpoint that allows remote attackers to upload malicious files by sending multipart POST requests with arbitrary filenames and disguised content types. Attackers can upload PHP webshells to the Document directory and execute them via HTTP GET requests to achieve remote code execution as the web server user. Exploitation evidence was first observed by the Shadowserver Foundation on 2022-10-10 (UTC). | 2026-04-30 | 9.8 | CVE-2022-50993 |
| xataboost--XATABoost CMS | XATABoost CMS 1.0.0 contains a union-based SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL | 2026-04-29 | 8.2 | CVE-2018-25300 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | code through the id parameter. Attackers can send GET requests to news.php with malicious id values to extract sensitive database information. | | | |
| YunaiV--yudao-cloud | A security flaw has been discovered in YunaiV yudao-cloud up to 2026.01. This impacts the function getAccessToken of the file yudao-module-system-biz/src/main/java/io/github/ruoyi/common/oauth2/service/impl/OAuth2TokenServiceImpl.java. Performing a manipulation results in improper authentication. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 7.3 | CVE-2026-7679 |
| YunaiV--yudao-cloud | A security flaw has been discovered in YunaiV yudao-cloud up to 3.8.0. This affects the function doFilterInternal of the file JwtAuthenticationTokenFilter.java of the component Ruoyi-Vue-Pro. Performing a manipulation of the argument mock-token results in improper authentication. 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. | 2026-05-03 | 7.3 | CVE-2026-7710 |
| Zyxel--DX3301-T0 firmware | A post-authentication command injection vulnerability in the "DomainName" parameter of the DHCP configuration file in Zyxel DX3301-T0 and EX3301-T0 firmware versions through 5.50(ABVY.7.1)C0 could allow an authenticated attacker with administrator privileges to execute OS commands on an affected device. | 2026-04-28 | 7.2 | CVE-2026-1460 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| AcademySoftware Foundation--openexr | OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. From 3.4.0 to before 3.4.9, a missing bounds check on the dataWindow attribute in EXR file headers allows an attacker to trigger a signed integer overflow in generic_unpack(). By setting dataWindow.min.x to a large negative value, OpenEXRCore computes an enormous image width, which is later used in a signed integer multiplication that overflows, causing the process to terminate with SIGILL via UBSan. This vulnerability is fixed in 3.4.9. | 2026-04-06 | 6.5 | CVE-2026-34378 |
| AcademySoftware Foundation--openexr | OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. From 3.2.0 to before 3.2.7, 3.3.9, and 3.4.9, a signed integer overflow exists in undo_pxr24_impl() in src/lib/OpenEXRCore/internal_pxr24.c at line 377. The expression (uint64_t)(w * 3) computes w * 3 as a signed 32-bit integer before casting to uint64_t. When w is large, this multiplication constitutes undefined behavior under the C standard. On tested builds (clang/gcc without sanitizers), two's-complement wraparound commonly occurs, and for specific values of w the wrapped result is a small positive integer, which may allow the subsequent bounds check to pass incorrectly. If the check is bypassed, the decoding loop proceeds to write pixel data through dout, potentially extending far beyond the allocated output buffer. This vulnerability is fixed in 3.2.7, 3.3.9, and 3.4.9. | 2026-04-06 | 5.9 | CVE-2026-34380 |
| addfunc--AddFunc Head & Footer Code | The AddFunc Head & Footer Code plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `aFhfc_head_code`, `aFhfc_body_code`, and `aFhfc_footer_code` post meta values in all versions up to, and including, 2.3. This is due to the plugin outputting these meta values without any sanitization or escaping. While the plugin restricts its own metabox and save handler to administrators via `current_user_can('manage_options')`, it does not use `register_meta()` with an `auth_callback` to protect these meta keys. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts via the WordPress Custom Fields interface that execute when an administrator previews or views the post. | 2026-04-10 | 6.4 | CVE-2026-2305 |
| Adivaha--WordPress adivaha Travel Plugin | WordPress adivaha Travel Plugin 2.3 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the isMobile parameter. Attackers can craft malicious URLs containing JavaScript payloads in the isMobile GET parameter at the /mobile-app/v3/ endpoint to execute arbitrary code in victims' browsers and steal session tokens or credentials. | 2026-04-09 | 6.1 | CVE-2023-54358 |
| arubadev--Aruba HiSpeed Cache | The Aruba HiSpeed Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0.4. This is due to missing nonce verification on the `ahsc_ajax_reset_options()` function. This makes it possible for unauthenticated attackers to reset all plugin settings to their default values via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 2026-04-10 | 4.3 | CVE-2026-1924 |
| blubrry--PowerPress Podcasting plugin by Blubrry | The Blubrry PowerPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'powerpress' and 'podcast' shortcodes in versions up to, and including, 11.15.15 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. | 2026-04-08 | 6.4 | CVE-2026-2988 |
| burlingtonbytes--WP Blockade Visual Page Builder | The WP Blockade plugin for WordPress is vulnerable to Missing Authorization in all versions up to and including 0.9.14. The plugin registers an admin_post action hook 'wp-blockade-shortcode-render' that maps to the render_shortcode_preview() function. This function lacks any capability check (current_user_can()) and nonce verification, allowing any authenticated user to execute arbitrary WordPress | 2026-04-08 | 6.5 | CVE-2026-3480 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | shortcodes. The function takes a user-supplied 'shortcode' parameter from $_GET, passes it through stripslashes(), and directly executes it via do_shortcode(). This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes, which could lead to information disclosure, privilege escalation, or other impacts depending on what shortcodes are registered on the site (e.g., shortcodes from other plugins that display sensitive data, perform actions, or include files). | | | |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 2.0.0-RC.3, an Insecure Direct Object Reference (IDOR) vulnerability in the REST API stats endpoint allows any authenticated user (including low-privilege students with ROLE_USER) to read any other user's learning progress, certificates, and gradebook scores for any course, without enrollment or supervisory relationship. This vulnerability is fixed in 2.0.0-RC.3. | 2026-04-10 | 6.5 | CVE-2026-33141 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38, the get_user_info_from_username REST API endpoint returns personal information (email, first name, last name, user ID, active status) of any user to any authenticated user, including students. There is no authorization check. This vulnerability is fixed in 1.11.38. | 2026-04-10 | 6.5 | CVE-2026-33708 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 2.0.0-RC.3, any authenticated user (including ROLE_STUDENT) can enumerate all platform users and access personal information (email, phone, roles) via GET /api/users, including administrator accounts. This vulnerability is fixed in 2.0.0-RC.3. | 2026-04-10 | 6.5 | CVE-2026-33736 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 2.0.0-RC.3, a Reflected Cross-Site Scripting (XSS) vulnerability in the exercise question list admin panel allows an attacker to execute arbitrary JavaScript in an authenticated teacher's browser. The pagination code merges all $_GET parameters via array_merge() and outputs the result via http_build_query() directly into HTML href attributes without htmlspecialchars() encoding. This vulnerability is fixed in 2.0.0-RC.3. | 2026-04-10 | 5.4 | CVE-2026-32893 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38, Twig template files (.tpl) under /main/template/default/ are directly accessible without authentication via HTTP GET requests. These templates expose internal application logic, variable names, AJAX endpoint URLs, and admin panel structure. This vulnerability is fixed in 1.11.38. | 2026-04-10 | 5.3 | CVE-2026-33705 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, multiple files use simplexml_load_string() without XXE protection. With LIBXML_NOENT flag, arbitrary server files can be read. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3. | 2026-04-10 | 5.3 | CVE-2026-33737 |
| chamilo--chamilo-lms | Chamilo LMS is a learning management system. Prior to 1.11.38 and 2.0.0-RC.3, an Open Redirect vulnerability in the session course edit page allows an attacker to redirect an authenticated administrator to an arbitrary external URL after saving coach assignment changes. The redirect also leaks the id_session parameter to the attacker's server. This vulnerability is fixed in 1.11.38 and 2.0.0-RC.3. | 2026-04-10 | 4.7 | CVE-2026-32932 |
| danny-avila--LibreChat | LibreChat is a ChatGPT clone with additional features. Prior to 0.8.4, LibreChat trusts the name field returned by the execute_code sandbox when persisting code-generated artifacts. On deployments using the default local file strategy, a malicious artifact filename containing traversal sequences (for example, ../../../../../app/client/dist/poc.txt) is concatenated into the server-side destination path and written with fs.writeFileSync() without sanitization. This gives any user who can trigger execute_code an arbitrary file write primitive as the LibreChat server user. This vulnerability is fixed in 0.8.4. | 2026-04-07 | 6.3 | CVE-2026-34371 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| David Lingren--Media LIbrary Assistant | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Lingren Media LIbrary Assistant allows Stored XSS.This issue affects Media LIbrary Assistant: from n/a through 3.34. | 2026-04-06 | 6.5 | CVE-2026-34897 |
| Dynalon--MDwiki | MDwiki contains a cross-site scripting vulnerability that allows remote attackers to execute arbitrary JavaScript by injecting malicious code through the location hash parameter. Attackers can craft URLs with JavaScript payloads in the hash fragment that are parsed and rendered without sanitization, causing the injected scripts to execute in the victim's browser context. | 2026-04-12 | 6.1 | CVE-2017-20239 |
| Elastic--Kibana | Server-Side Request Forgery (CWE-918) in Kibana One Workflow can lead to information disclosure. An authenticated user with workflow creation and execution privileges can bypass host allowlist restrictions in the Workflows Execution Engine, potentially exposing sensitive internal endpoints and data. | 2026-04-08 | 6.8 | CVE-2026-33458 |
| Elastic--Kibana | Uncontrolled Resource Consumption (CWE-400) in Kibana can lead to denial of service via Excessive Allocation (CAPEC-130). An authenticated user with access to the automatic import feature can submit specially crafted requests with excessively large input values. When multiple such requests are sent concurrently, the backend services become unstable, resulting in service disruption and deployment unavailability for all users. | 2026-04-08 | 6.5 | CVE-2026-33459 |
| Elastic--Kibana | Incorrect Authorization (CWE-863) in Kibana can lead to cross-space information disclosure via Privilege Abuse (CAPEC-122). A user with Fleet agent management privileges in one Kibana space can retrieve Fleet Server policy details from other spaces through an internal enrollment endpoint. The endpoint bypasses space-scoped access controls by using an unscoped internal client, returning operational identifiers, policy names, management state, and infrastructure linkage details from spaces the user is not authorized to access. | 2026-04-08 | 4.3 | CVE-2026-33460 |
| electron--electron | Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.5, 40.8.5, 41.1.0, and 42.0.0-alpha.5, when a renderer calls window.open() with a target name, Electron did not correctly scope the named-window lookup to the opener's browsing context group. A renderer could navigate an existing child window that was opened by a different, unrelated renderer if both used the same target name. If that existing child was created with more permissive webPreferences (via setWindowOpenHandler's overrideBrowserWindowOptions), content loaded by the second renderer inherits those permissions. Apps are only affected if they open multiple top-level windows with differing trust levels and use setWindowOpenHandler to grant child windows elevated webPreferences such as a privileged preload script. Apps that do not elevate child window privileges, or that use a single top-level window, are not affected. Apps that additionally grant nodeIntegration: true or sandbox: false to child windows (contrary to the security recommendations) may be exposed to arbitrary code execution. This vulnerability is fixed in 39.8.5, 40.8.5, 41.1.0, and 42.0.0-alpha.5. | 2026-04-07 | 6 | CVE-2026-34765 |
| elemntor--Elementor Website Builder more than just a page builder | The Elementor Website Builder - More Than Just a Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several widget parameters in all versions up to, and including, 3.35.5 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. | 2026-04-08 | 6.4 | CVE-2025-14732 |
| Eniture technology--LTL Freight Quotes Worldwide Express Edition | Missing Authorization vulnerability in Eniture technology LTL Freight Quotes - Worldwide Express Edition allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects LTL Freight Quotes - Worldwide Express Edition: from n/a through 5.2.1. | 2026-04-07 | 5.3 | CVE-2026-34899 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| fernandobt--List category posts | The List category posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'catlist' shortcode in all versions up to, and including, 0.94.0 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. | 2026-04-09 | 6.4 | CVE-2026-3005 |
| GitLab--GitLab | GitLab has remediated an issue in GitLab EE affecting all versions from 18.2 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that could have allowed an authenticated user to cause denial of service to the GitLab instance due to improper input validation in GraphQL queries. | 2026-04-08 | 6.5 | CVE-2026-1101 |
| GitLab--GitLab | GitLab has remediated an issue in GitLab EE affecting all versions from 18.0.0 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that in Code Quality reports could have allowed an authenticated user to leak IP addresses of users viewing the report via specially crafted content. | 2026-04-08 | 5.7 | CVE-2026-1516 |
| GitLab--GitLab | GitLab has remediated an issue in GitLab EE affecting all versions from 16.6 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that under certain circumstances could have allowed an authenticated user to have access to other users' email addresses via certain GraphQL queries. | 2026-04-08 | 4.3 | CVE-2025-9484 |
| GitLab--GitLab | GitLab has remediated an issue in GitLab EE affecting all versions from 11.3 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that could have allowed an authenticated user with developer-role permissions to modify protected environment settings due to improper authorization checks in the API. | 2026-04-08 | 4.3 | CVE-2026-1752 |
| GitLab--GitLab | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.2 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3 that could have allowed an authenticated user to access confidential issues assigned to other users via CSV export due to insufficient authorization checks. | 2026-04-08 | 4.3 | CVE-2026-2104 |
| HDFGroup--hdf5 | HDF5 is software for managing data. In 1.14.1-2 and earlier, an attacker who can control an h5 file parsed by HDF5 can trigger a write-based heap buffer overflow condition in the H5T__ref_mem_setnull method. This can lead to a denial-of-service condition, and potentially further issues such as remote code execution depending on the practical exploitability of the heap overflow against modern operating systems. | 2026-04-10 | 5.5 | CVE-2026-29043 |
| Heatmiser--Heatmiser Wifi Thermostat | Heatmiser Wifi Thermostat 1.7 contains a cross-site request forgery vulnerability that allows attackers to change administrator credentials by tricking authenticated users into submitting malicious requests. Attackers can craft HTML forms targeting the networkSetup.htm endpoint with parameters usnm, usps, and cfps to modify the admin username and password without user consent. | 2026-04-12 | 4.3 | CVE-2019-25708 |
| Hikashop--Joomla HikaShop | Joomla HikaShop 4.7.4 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating GET parameters in the product filter endpoint. Attackers can craft malicious URLs containing XSS payloads in the from_option, from_ctrl, from_task, or from_itemid parameters to steal session tokens or login credentials when victims visit the link. | 2026-04-09 | 6.1 | CVE-2023-54364 |
| Hitachi--JP1/IT Desktop Management 2 - Manager | Buffer Overflow Vulnerability in JP1/IT Desktop Management 2 - Manager on Windows, JP1/IT Desktop Management 2 - Operations Director on Windows, Job Management Partner 1/IT Desktop Management 2 - Manager on Windows, JP1/IT Desktop Management - Manager on Windows, Job Management Partner 1/IT Desktop Management - Manager on Windows, JP1/NETM/DM Manager on Windows, JP1/NETM/DM Client on Windows, Job Management Partner 1/Software Distribution Manager on Windows, Job Management Partner 1/Software Distribution Client on Windows.This issue affects JP1/IT Desktop Management 2 - Manager: from 13-50 before 13-50-02, from 13-11 before 13-11-04, from 13-10 before 13-10-07, from 13-01 before 13-01-07, from 13-00 before 13-00-05, from 12-60 before 12-60-12, from 10-50 through 12-50-11; JP1/IT Desktop Management | 2026-04-07 | 5.5 | CVE-2025-65116 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | 2 - Operations Director: from 13-50 before 13-50-02, from 13-11 before 13-11-04, from 13-10 before 13-10-07, from 13-01 before 13-01-07, from 13-00 before 13-00-05, from 12-60 before 12-60-12, from 10-50 through 12-50-11; Job Management Partner 1/IT Desktop Management 2 - Manager: from 10-50 through 10-50-11; JP1/IT Desktop Management - Manager: from 09-50 through 10-10-16; Job Management Partner 1/IT Desktop Management - Manager: from 09-50 through 10-10-16; JP1/NETM/DM Manager: from 09-00 through 10-20-02; JP1/NETM/DM Client: from 09-00 through 10-20-02; Job Management Partner 1/Software Distribution Manager: from 09-00 through 09-51-13; Job Management Partner 1/Software Distribution Client: from 09-00 through 09-51-13. | | | |
| homarr-labs--homarr | Homarr is an open-source dashboard. Prior to 1.57.0, the user registration endpoint (/api/trpc/user.register) is vulnerable to a race condition that allows an attacker to create multiple user accounts from a single-use invite token. The registration flow performs three sequential database operations without a transaction: CHECK, CREATE, and DELETE. Because these operations are not atomic, concurrent requests can all pass the validation step (1) before any of them reaches the deletion step (3). This allows multiple accounts to be registered using a single invite token that was intended to be single-use. This vulnerability is fixed in 1.57.0. | 2026-04-06 | 4.2 | CVE-2026-32602 |
| IBM--Concert | IBM Concert 1.0.0 through 2.2.0 creates temporary files with predictable names, which allows local users to overwrite arbitrary files via a symlink attack. | 2026-04-07 | 6.2 | CVE-2025-13044 |
| idealwebdesignlk--Whole Enquiry Cart for WooCommerce | The Whole Enquiry Cart for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'woowhole_success_msg' parameter in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, 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. | 2026-04-08 | 4.4 | CVE-2026-2838 |
| inisev--BackupBliss Backup & Migration with Free Cloud Storage | The Backup Migration plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 2.0.0. This is due to a missing capability check on the 'initializeOfflineAjax' function and lack of proper nonce verification. The endpoint only validates against hardcoded tokens which are publicly exposed in the plugin's JavaScript. This makes it possible for unauthenticated attackers to trigger the backup upload queue processing, potentially causing unexpected backup transfers to configured cloud storage targets and resource exhaustion. | 2026-04-07 | 5.3 | CVE-2025-14944 |
| Jlexart--Joomla JLex Review | Joomla JLex Review 6.0.1 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the review_id URL parameter. Attackers can craft malicious links containing JavaScript payloads that execute in victims' browsers when clicked, enabling session hijacking or credential theft. | 2026-04-09 | 6.1 | CVE-2023-54360 |
| johanaarstein--AM LottiePlayer | The AM LottiePlayer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via uploaded SVG files in all versions up to, and including, 3.6.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 2026-04-08 | 5.4 | CVE-2025-1794 |
| Juniper Networks--JSI LWC | A Permissive List of Allowed Input vulnerability in the CLI of Juniper Networks Support Insights (JSI) Virtual Lightweight Collector (vLWC) allows a local, high privileged attacker to escalate their privileges to root. The CLI menu accepts input without carefully validating it, which allows for shell command injection. These shell commands are executed with root permissions and can be used to gain complete control of the system. This issue affects all JSI vLWC versions before 3.0.94. | 2026-04-09 | 6.7 | CVE-2026-21915 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Juniper Networks--Junos OS | A Missing Authentication for Critical Function vulnerability in command processing of Juniper Networks Junos OS allows a privileged local attacker to gain access to line cards running Junos OS Evolved as root. This issue affects systems running Junos OS using Linux-based line cards. Affected line cards include: * MPC7, MPC8, MPC9, MPC10, MPC11 * LC2101, LC2103 * LC480, LC4800, LC9600 * MX304 (built-in FPC) * MX-SPC3 * SRX5K-SPC3 * EX9200-40XS * FPC3-PTX-U2, FPC3-PTX-U3 * FPC3-SFF-PTX * LC1101, LC1102, LC1104, LC1105 This issue affects Junos OS: * all versions before 22.4R3-S8, * from 23.2 before 23.2R2-S6, * from 23.4 before 23.4R2-S6, * from 24.2 before 24.2R2-S3, * from 24.4 before 24.4R2, * from 25.2 before 25.2R2. | 2026-04-08 | 6.7 | CVE-2025-30650 |
| Juniper Networks--Junos OS | An Incorrect Synchronization vulnerability in the management daemon (mgd) of Juniper Networks Junos OS and Junos OS Evolved allows a network-based attacker with low privileges to cause a complete Denial-of-Service (DoS) of the management plane. When NETCONF sessions are quickly established and disconnected, a locking issue causes mgd processes to hang in an unusable state. When the maximum number of mgd processes has been reached, no new logins are possible. This leads to the inability to manage the device and requires a power-cycle to recover. This issue can be monitored by checking for mgd processes in lockf state in the output of 'show system processes extensive': user@host> show system processes extensive \| match mgd <pid> root 20 0 501M 4640K lockf 1 0:01 0.00% mgd If the system still can be accessed (either via the CLI or as root, which might still be possible as last resort as this won't invoke mgd), mgd processes in this state can be killed with 'request system process terminate <PID>' from the CLI or with 'kill -9 <PID>' from the shell. This issue affects: Junos OS: * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R2-S1, * 24.4 versions before 24.4R1-S3, 24.4R2; This issue does not affect Junos OS versions before 23.4R1; Junos OS Evolved: * 23.4 versions before 23.4R2-S5-EVO, * 24.2 versions before 24.2R2-S1-EVO, * 24.4 versions before 24.4R1-S3-EVO, 24.4R2-EVO. This issue does not affect Junos OS Evolved versions before 23.4R1-EVO; | 2026-04-09 | 6.5 | CVE-2026-21919 |
| 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 an unauthenticated, network-based attacker to bypass the configured firewall filter and access the control-plane of the device. On MX platforms with MPC10, MPC11, LC4800 or LC9600 line cards, and MX304, firewall filters applied on a loopback interface lo0.n (where n is a non-0 number) don't get executed when lo0.n is in the global VRF / default routing-instance. An affected configuration would be: user@host# show configuration interfaces lo0 \| display set set interfaces lo0 unit 1 family inet filter input <filter-name> where a firewall filter is applied to a non-0 loopback interface, but that loopback interface is not referred to in any routing-instance (RI) configuration, which implies that it's used in the default RI. The issue can be observed with the CLI command: user@device> show firewall counter filter <filter_name> not showing any matches. 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, * 24.4 versions before 24.4R2. | 2026-04-09 | 6.5 | CVE-2026-33774 |
| Juniper Networks--Junos OS | A Missing Release of Memory after Effective Lifetime vulnerability in the BroadBand Edge subscriber management daemon (bbe-smgd) of Juniper Networks Junos OS on MX Series allows an adjacent, unauthenticated attacker to cause a Denial of Service (DoS). If the authentication packet-type option is configured and a received packet does not match that packet type, the memory leak occurs. When all memory available to bbe-smgd has been consumed, no new subscribers will be able to login. The memory utilization of bbe-smgd can be monitored with the following show command: user@host> show system processes extensive \| match bbe-smgd The below log message can be observed when this limit has been reached: bbesmgd[<PID>]: %DAEMON-3-SMD_DPROF_RSMON_ERROR: Resource unavailability, Reason: Daemon Heap Memory exhaustion This issue affects Junos OS on MX Series: * all versions before 22.4R3-S8, * 23.2 versions before 23.2R2-S5, | 2026-04-09 | 6.5 | CVE-2026-33775 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | * 23.4 versions before 23.4R2-S6, * 24.2 versions before 24.2R2-S2, * 24.4 versions before 24.4R2, * 25.2 versions before 25.2R2. | | | |
| Juniper Networks--Junos OS | An Improper Following of a Certificate's Chain of Trust vulnerability in J-Web of Juniper Networks Junos OS on SRX Series allows a PITM to intercept the communication of the device and get access to confidential information and potentially modify it. When an SRX device is provisioned to connect to Security Director (SD) cloud, it doesn't perform sufficient verification of the received server certificate. This allows a PITM to intercept the communication between the SRX and SD cloud and access credentials and other sensitive information. This issue affects Junos OS: * all versions before 22.4R3-S9, * 23.2 versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S7, * 24.2 versions before 24.2R2-S3, * 24.4 versions before 24.4R2-S2, * 25.2 versions before 25.2R1-S2, 25.2R2. | 2026-04-09 | 6.5 | CVE-2026-33779 |
| Juniper Networks--Junos OS | A Missing Release of Memory after Effective Lifetime vulnerability in the Layer 2 Address Learning Daemon (l2ald) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent, unauthenticated attacker to cause a memory leak ultimately leading to a Denial of Service (DoS). In an EVPN-MPLS scenario, routes learned from remote multi-homed Provider Edge (PE) devices are programmed as ESI routes. Due to a logic issue in the l2ald memory management, memory allocated for these routes is not released when there is churn for these routes. As a result, memory leaks in the l2ald process which will ultimately lead to a crash and restart of l2ald. Use the following command to monitor the memory consumption by l2ald: user@device> show system process extensive \| match "PID\|l2ald" This issue affects: Junos OS: * all versions before 22.4R3-S5, * 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R2; Junos OS Evolved: * all versions before 22.4R3-S5-EVO, * 23.2 versions before 23.2R2-S3-EVO, * 23.4 versions before 23.4R2-S4-EVO, * 24.2 versions before 24.2R2-EVO. | 2026-04-09 | 6.5 | CVE-2026-33780 |
| 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 specific EX and QFX Series devices allow an unauthenticated, adjacent attacker to cause a complete Denial of Service (DoS). On EX4k, and QFX5k platforms configured as service-provider edge devices, if L2PT is enabled on the UNI and VSTP is enabled on NNI in VXLAN scenarios, receiving VSTP BPDUs on UNI leads to packet buffer allocation failures, resulting in the device to not pass traffic anymore until it is manually recovered with a restart.This issue affects Junos OS: * 24.4 releases before 24.4R2, * 25.2 releases before 25.2R1-S1, 25.2R2. This issue does not affect Junos OS releases before 24.4R1. | 2026-04-09 | 6.5 | CVE-2026-33781 |
| Juniper Networks--Junos OS | A Missing Release of Memory after Effective Lifetime vulnerability in the DHCP daemon (jdhcpd) of Juniper Networks Junos OS on MX Series, allows an adjacent, unauthenticated attacker to cause a memory leak, that will eventually cause a complete Denial-of-Service (DoS). In a DHCPv6 over PPPoE, or DHCPv6 over VLAN with Active lease query or Bulk lease query scenario, every subscriber logout will leak a small amount of memory. When all available memory has been exhausted, jdhcpd will crash and restart which causes a complete service impact until the process has recovered. The memory usage of jdhcpd can be monitored with: user@host> show system processes extensive \| match jdhcpd This issue affects Junos OS: * all versions before 22.4R3-S1, * 23.2 versions before 23.2R2, * 23.4 versions before 23.4R2. | 2026-04-09 | 6.5 | CVE-2026-33782 |
| Juniper Networks--Junos OS | An OS Command Injection vulnerability in the CLI processing of Juniper Networks Junos OS and Junos OS Evolved allows a local, high-privileged attacker executing specific, crafted CLI commands to inject arbitrary shell commands as root, leading to a complete compromise of the system. Certain 'set system' commands, when executed with crafted arguments, are not properly sanitized, allowing for arbitrary shell injection. These shell commands are executed as root, potentially allowing for complete control of the vulnerable system. This issue affects: Junos OS: * all versions before 22.4R3-S8, * from 23.2 before 23.2R2-S5, * from 23.4 before 23.4R2-S7, * from 24.2 before 24.2R2-S2, * from 24.4 before 24.4R2, * from 25.2 | 2026-04-09 | 6.7 | CVE-2026-33791 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | before 25.2R2; Junos OS Evolved: * all versions before 22.4R3-S8-EVO, * from 23.2 before 23.2R2-S5-EVO, * from 23.4 before 23.4R2-S7-EVO, * from 24.2 before 24.2R2-S2-EVO, * from 24.4 before 24.4R2-EVO, * from 25.2 before 25.2R1-S1-EVO, 25.2R2-EVO. | | | |
| Juniper Networks--Junos OS | An Incorrect Initialization of Resource vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on specific EX Series and QFX Series device allows an unauthenticated, network-based attacker to cause an integrity impact to downstream networks. When the same family inet or inet6 filter is applied on an IRB interface and on a physical interface as egress filter on EX4100, EX4400, EX4650 and QFX5120 devices, only one of the two filters will be applied, which can lead to traffic being sent out one of these interfaces which should have been blocked. This issue affects Junos OS on EX Series and QFX Series: * 23.4 version 23.4R2-S6, * 24.2 version 24.2R2-S3. No other Junos OS versions are affected. | 2026-04-09 | 5.8 | CVE-2026-33773 |
| Juniper Networks--Junos OS | A Missing Authorization vulnerability in the CLI of Juniper Networks Junos OS and Junos OS Evolved allows a local user with low privileges to read sensitive information. A local user with low privileges can execute the CLI command 'show mgd' with specific arguments which will expose sensitive information. This issue affects Junos OS: * all versions before 22.4R3-S8, * 23.2 versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S6, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S1, * 25.2 version before 25.2R1-S2, 25.2R2; Junos OS Evolved: * all versions before 23.2R2-S6-EVO, * 23.4 version before 23.4R2-S6-EVO, * 24.2 version before 24.2R2-S4-EVO, * 24.4 versions before 24.4R2-S1-EVO, * 25.2 versions before 25.2R2-EVO. | 2026-04-09 | 5.5 | CVE-2026-33776 |
| Juniper Networks--Junos OS | An Improper Check for Unusual or Exceptional Conditions vulnerability in the chassis control daemon (chassisd) of Juniper Networks Junos OS on SRX1600, SRX2300 and SRX4300 allows a local attacker with low privileges to cause a complete Denial of Service (DoS). When a specific 'show chassis' CLI command is executed, chassisd crashes and restarts which causes a momentary impact to all traffic until all modules are online again. This issue affects Junos OS on SRX1600, SRX2300 and SRX4300: * 24.4 versions before 24.4R1-S3, 24.4R2. This issue does not affect Junos OS versions before 24.4R1. | 2026-04-09 | 5.5 | CVE-2026-33786 |
| Juniper Networks--Junos OS | An Improper Check for Unusual or Exceptional Conditions vulnerability in the chassis control daemon (chassisd) of Juniper Networks Junos OS on SRX1500, SRX4100, SRX4200 and SRX4600 allows a local attacker with low privileges to cause a complete Denial of Service (DoS). When a specific 'show chassis' CLI command is executed, chassisd crashes and restarts which causes a momentary impact to all traffic until all modules are online again. This issue affects Junos OS on SRX1500, SRX4100, SRX4200 and SRX4600: * 23.2 versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S7 * 24.2 versions before 24.2R2-S2, * 24.4 versions before 24.4R2, * 25.2 versions before 25.2R1-S1, 25.2R2. | 2026-04-09 | 5.5 | CVE-2026-33787 |
| Juniper Networks--Junos OS Evolved | A Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in the advanced forwarding toolkit (evo-aftmand/evo-pfemand) of Juniper Networks Junos OS Evolved on PTX Series or QFX5000 Series allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS).An attacker sending crafted multicast packets will cause line cards running evo-aftmand/evo-pfemand to crash and restart or non-line card devices to crash and restart. Continued receipt and processing of these packets will sustain the Denial of Service (DoS) condition. This issue affects Junos OS Evolved PTX Series: * All versions before 22.4R3-S8-EVO, * from 23.2 before 23.2R2-S5-EVO, * from 23.4 before 23.4R2-EVO, * from 24.2 before 24.2R2-EVO, * from 24.4 before 24.4R2-EVO. This issue affects Junos OS Evolved on QFX5000 Series: * 22.2-EVO version before 22.2R3-S7-EVO, * 22.4-EVO version before 22.4R3-S7-EVO, * 23.2-EVO versions before 23.2R2-S4-EVO, * 23.4-EVO versions before 23.4R2-S5-EVO, * 24.2-EVO versions before 24.2R2-S1-EVO, * 24.4-EVO versions before 24.4R1-S3-EVO, 24.4R2-EVO. This issue does not affect Junos OS Evolved on QFX5000 Series | 2026-04-09 | 6.5 | CVE-2025-59969 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | versions before: 21.2R2-S1-EVO, 21.2R3-EVO, 21.3R2-EVO, 21.4R1-EVO, and 22.1R1-EVO. | | | |
| Juniper Networks--Junos OS Evolved | A Function Call With Incorrect Argument Type vulnerability in the sensor interface of Juniper Networks Junos OS Evolved on PTX Series allows a network-based, authenticated attacker with low privileges to cause a complete Denial of Service (DoS). If colored SRTE policy tunnels are provisioned via PCEP, and gRPC is used to monitor traffic in these tunnels, evo-aftmand crashes and doesn't restart which leads to a complete and persistent service impact. The system has to be manually restarted to recover. The issue is seen only when the Originator ASN field in PCEP contains a value larger than 65,535 (32-bit ASN). The issue is not reproducible when SRTE policy tunnels are statically configured. This issue affects Junos OS Evolved on PTX Series: * all versions before 22.4R3-S9-EVO, * 23.2 versions before 23.2R2-S6-EVO, * 23.4 versions before 23.4R2-S7-EVO, * 24.2 versions before 24.2R2-S4-EVO, * 24.4 versions before 24.4R2-S2-EVO, * 25.2 versions before 25.2R1-S2-EVO, 25.2R2-EVO. | 2026-04-09 | 6.5 | CVE-2026-33783 |
| Juniper Networks--Junos Space | An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the list filter field that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator. This issue affects all versions of Junos Space before 24.1R5 Patch V3. | 2026-04-09 | 6.1 | CVE-2026-21904 |
| magicplugins--Magic Conversation For Gravity Forms | The Magic Conversation For Gravity Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'magic-conversation' shortcode in all versions up to, and including, 3.0.97 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. | 2026-04-08 | 6.4 | CVE-2026-1396 |
| Microsoft--Microsoft Edge (Chromium-based) | Microsoft Edge (Chromium-based) Spoofing Vulnerability | 2026-04-10 | 4.3 | CVE-2026-33118 |
| Microsoft--Microsoft Edge for Android | User interface (ui) misrepresentation of critical information in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network. | 2026-04-10 | 5.4 | CVE-2026-33119 |
| n/a--Intel(R) Pentium(R) Processor Silver Series, Intel(R) Celeron(R) Processor J Series, Intel(R) Celeron(R) Processor N Series may allow an escalation of privilege. Hardware reverse engineer adversary with a privileged user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via physical access | Use of Default Cryptographic Key in the hardware for some Intel(R) Pentium(R) Processor Silver Series, Intel(R) Celeron(R) Processor J Series, Intel(R) Celeron(R) Processor N Series may allow an escalation of privilege. Hardware reverse engineer adversary with a privileged user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via physical access when attack requirements are present with special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (high), integrity (high) and availability (none) impacts. | 2026-04-08 | 6.6 | CVE-2026-20709 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| when attack requirements are present with special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (high), integrity (high) and availability (none) impacts. | | | | |
| NSauditor--BlueAuditor | BlueAuditor 1.7.2.0 contains a buffer overflow vulnerability in the registration key field that allows local attackers to crash the application by submitting an oversized key value. Attackers can trigger a denial of service by entering a 256-byte buffer of repeated characters in the Key registration field, causing the application to crash during registration processing. | 2026-04-12 | 6.2 | CVE-2019-25712 |
| NSauditor--SpotFTP Password Recover | SpotFTP Password Recover 2.4.2 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an oversized buffer in the Name field during registration. Attackers can generate a 256-byte payload, paste it into the Name input field, and trigger a crash when submitting the registration code. | 2026-04-12 | 6.2 | CVE-2019-25711 |
| OceanWP--Ocean Extra | Missing Authorization vulnerability in OceanWP Ocean Extra allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ocean Extra: from n/a through 2.5.3. | 2026-04-07 | 5.4 | CVE-2026-34903 |
| OCS Inventory--OCS Inventory NG Server | OCS Inventory NG Server version 2.12.3 and prior contain a stored cross-site scripting vulnerability that allows unauthenticated attackers to execute arbitrary JavaScript by submitting malicious User-Agent HTTP headers to the /ocsinventory endpoint. Attackers can register rogue agents or craft requests with malicious User-Agent values that are stored without sanitation and rendered with insufficient encoding in the web console, leading to arbitrary JavaScript execution in the browsers of authenticated users viewing the statistics dashboard. | 2026-04-06 | 5.4 | CVE-2026-22675 |
| opensourcepos--opensourcepos | Open Source Point of Sale is a web based point-of-sale application written in PHP using CodeIgniter framework. Prior to 3.4.3, a Stored Cross-Site Scripting (XSS) vulnerability exists in the Daily Sales management table. The customer_name column is configured with escape: false in the bootstrap-table column configuration, causing customer names to be rendered as raw HTML. An attacker with customer management permissions can inject arbitrary JavaScript into a customer's first_name or last_name field, which executes in the browser of any user viewing the Daily Sales page. This vulnerability is fixed in 3.4.3. | 2026-04-07 | 5.4 | CVE-2026-32712 |
| pi-hole--pi-hole | Pi-hole is a Linux network-level advertisement and Internet tracker blocking application. Version 6.4 has a local privilege-escalation vulnerability allows code execution as root from the low-privilege pihole account. Important context: the pihole account uses nologin, so this is not a direct interactive-login issue. However, | 2026-04-06 | 6.4 | CVE-2026-33727 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | nologin does not prevent code from running as UID pihole if a Pi-hole component is compromised. In that realistic post-compromise scenario, attacker-controlled content in /etc/pihole/versions is sourced by root-run Pi-hole scripts, leading to root code execution. This vulnerability is fixed in 6.4.1. | | | |
| pi-hole--web | Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. From 6.0 to before 6.5, a reflected DOM-based XSS vulnerability in taillog.js allows an unauthenticated attacker to inject arbitrary HTML into the Pi-hole admin interface by crafting a malicious URL. The file query parameter is interpolated into an innerHTML assignment without escaping. Because the Content-Security-Policy is missing the form-action directive, injected <form> elements can exfiltrate credentials to an external origin. This vulnerability is fixed in 6.5. | 2026-04-06 | 6.1 | CVE-2026-33403 |
| pi-hole--web | Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. From 6.0 to before 6.5, configuration values from the /api/config endpoint are placed directly into HTML value="" attributes without escaping in settings-advanced.js, enabling HTML attribute injection. A double quote in any config value breaks out of the attribute context. JavaScript execution is blocked by the server's CSP (script-src 'self'), but injected attributes can alter element styling for UI redressing. The primary attack vector is importing a malicious teleporter backup, which bypasses per-field server-side validation. This vulnerability is fixed in 6.5. | 2026-04-06 | 5.4 | CVE-2026-33406 |
| pnggroup--libpng | LIBPNG is a reference library for use in applications that read, create, and manipulate PNG (Portable Network Graphics) raster image files. From 1.0.9 to before 1.6.57, passing a pointer obtained from png_get_PLTE, png_get_tRNS, or png_get_hIST back into the corresponding setter on the same png_struct/png_info pair causes the setter to read from freed memory and copy its contents into the replacement buffer. The setter frees the internal buffer before copying from the caller-supplied pointer, which now dangles. The freed region may contain stale data (producing silently corrupted chunk metadata) or data from subsequent heap allocations (leaking unrelated heap contents into the chunk struct). This vulnerability is fixed in 1.6.57. | 2026-04-09 | 5.1 | CVE-2026-34757 |
| posimyththemes--The Plus Addons for Elementor Addons for Elementor, Page Templates, Widgets, Mega Menu, WooCommerce | The The Plus Addons for Elementor - Addons for Elementor, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Progress Bar shortcode in all versions up to, and including, 6.4.9 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. | 2026-04-08 | 6.4 | CVE-2026-3311 |
| projectzealous01--PZ Frontend Manager | The PZ Frontend Manager plugin for WordPress is vulnerable to Missing Authorization in all versions up to and including 1.0.6. The pzfm_user_request_action_callback() function, registered via the wp_ajax_pzfm_user_request_action action hook, lacks both capability checks and nonce verification. This function handles user activation, deactivation, and deletion operations. When the 'dataType' parameter is set to 'delete', the function calls wp_delete_user() on all provided user IDs without verifying that the current user has the appropriate permissions. Notably, the similar pzfm_remove_item_callback() function does check pzfm_can_delete_user() before performing deletions, indicating this was an oversight. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary WordPress users (including administrators) by sending a crafted request to the AJAX endpoint. | 2026-04-08 | 5.3 | CVE-2026-3477 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Qualcomm, Inc.--Snapdragon | Memory Corruption when accessing freed memory due to concurrent fence deregistration and signal handling. | 2026-04-06 | 6.5 | CVE-2025-47374 |
| realmag777--BEAR Bulk Editor and Products Manager Professional for WooCommerce by Pluginus.Net | The BEAR - Bulk Editor and Products Manager Professional for WooCommerce by Pluginus.Net plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.5. This is due to missing nonce validation on the woobe_redraw_table_row() function. This makes it possible for unauthenticated attackers to update WooCommerce product data including prices, descriptions, and other product fields via a forged request granted they can trick a site administrator or shop manager into performing an action such as clicking on a link. | 2026-04-08 | 6.5 | CVE-2026-1672 |
| realmag777--BEAR Bulk Editor and Products Manager Professional for WooCommerce by Pluginus.Net | The BEAR - Bulk Editor and Products Manager Professional for WooCommerce by Pluginus.Net plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.5. This is due to missing nonce validation on the woobe_delete_tax_term() function. This makes it possible for unauthenticated attackers to delete WooCommerce taxonomy terms (categories, tags, etc.) via a forged request granted they can trick a site administrator or shop manager into performing an action such as clicking on a link. | 2026-04-08 | 4.3 | CVE-2026-1673 |
| Red Hat--mirror registry for Red Hat OpenShift | A flaw was found in the OpenShift Mirror Registry. This vulnerability allows an unauthenticated, remote attacker to enumerate valid usernames and email addresses via different error messages during authentication failures and account creation. | 2026-04-08 | 5.3 | CVE-2025-14243 |
| Red Hat--mirror registry for Red Hat OpenShift | A flaw was found in Red Hat Quay's Proxy Cache configuration feature. When an organization administrator configures an upstream registry for proxy caching, Quay makes a network connection to the specified registry hostname without verifying that it points to a legitimate external service. An attacker with organization administrator privileges could supply a crafted hostname to force the Quay server to make requests to internal network services, cloud infrastructure endpoints, or other resources that should not be accessible from the Quay application. | 2026-04-08 | 5.2 | CVE-2026-32591 |
| Red Hat--Multicluster Engine for Kubernetes | A container privilege escalation flaw was found in certain Multicluster Engine for Kubernetes images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container. | 2026-04-08 | 6.4 | CVE-2025-57851 |
| Red Hat--Red Hat Ansible Automation Platform 2 | A container privilege escalation flaw was found in certain Ansible Automation Platform images. This issue arises from the /etc/passwd file being created with group-writable permissions during the build process. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the /etc/passwd file. This vulnerability allows an attacker to add a new user with any arbitrary UID, including UID 0, gaining full root privileges within the container. | 2026-04-08 | 6.4 | CVE-2025-57847 |
| Red Hat--Red Hat OpenShift Update Service | A container privilege escalation flaw was found in certain OpenShift Update Service (OSUS) images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, may be able to leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container. | 2026-04-08 | 6.4 | CVE-2025-57854 |
| Red Hat--Red Hat Process Automation 7 | A container privilege escalation flaw was found in certain Red Hat Process Automation Manager images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the | 2026-04-08 | 6.4 | CVE-2025-58713 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container. | | | |
| Red Hat--Red Hat Web Terminal | A container privilege escalation flaw was found in certain Web Terminal images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container. | 2026-04-08 | 6.4 | CVE-2025-57853 |
| Siklu--EtherHaul 8010 | Siklu EtherHaul 8010 siklu-uimage-nxp-enc-10_6_2-18707-ea552dc00b devices have a static root password. | 2026-04-08 | 6.4 | CVE-2025-57175 |
| smub--Charitable Donation Plugin for WordPress Fundraising with Recurring Donations & More | The Charitable - Donation Plugin for WordPress - Fundraising with Recurring Donations & More plugin for WordPress is vulnerable to Insufficient Verification of Data Authenticity in versions up to, and including, 1.8.9.7. This is due to missing cryptographic verification of incoming Stripe webhook events. This makes it possible for unauthenticated attackers to forge payment_intent.succeeded webhook payloads and mark pending donations as completed without a real payment. | 2026-04-07 | 5.3 | CVE-2026-3177 |
| Solidres--Joomla Solidres | Joomla Solidres 2.13.3 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating multiple GET parameters including show, reviews, type_id, distance, facilities, categories, prices, location, and Itemid. Attackers can craft malicious URLs containing JavaScript payloads in these parameters to steal session tokens, login credentials, or manipulate site content when victims visit the crafted links. | 2026-04-09 | 6.1 | CVE-2023-54363 |
| Synology--Synology SSL VPN Client | A files or directories accessible to external parties vulnerability in Synology SSL VPN Client before 1.4.5-0684 allows remote attackers to access files within the installation directory via a local HTTP server bound to the loopback interface. By leveraging user interaction with a crafted web page, attackers may retrieve sensitive files such as configuration files, certificates, and logs, leading to information disclosure. | 2026-04-10 | 6.5 | CVE-2021-47960 |
| themeum--Tutor LMS eLearning and online course solution | The Tutor LMS - eLearning and online course solution plugin for WordPress is vulnerable to unauthorized private course enrollment in all versions up to, and including, 3.9.7. This is due to missing post_status validation in the `enroll_now()` and `course_enrollment()` functions. Both enrollment endpoints verify the nonce, user authentication, and whether the course is purchasable, but fail to check if the course has a `private` post_status. This makes it possible for authenticated attackers with Subscriber-level access or above to enroll in private courses by sending a crafted POST request with the target course ID. The enrollment record is created in the database and the private course title and enrollment status are exposed in the subscriber's dashboard, though WordPress core access control prevents the subscriber from viewing the actual course content (returns 404). Enrollment in private courses should be restricted to users with the `read_private_posts` capability. | 2026-04-11 | 5.4 | CVE-2026-3358 |
| themeum--Tutor LMS eLearning and online course solution | The Tutor LMS - eLearning and online course solution plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.9.7. This is due to missing authorization checks in the `save_course_content_order()` private method, which is called unconditionally by the `tutor_update_course_content_order` AJAX handler. While the handler's `content_parent` branch includes a `can_user_manage()` check, the `save_course_content_order()` call processes attacker-supplied `tutor_topics_lessons_sorting` JSON without any ownership or capability verification. This makes it possible for authenticated attackers with Subscriber-level access or above to detach lessons from topics, reorder course content, and | 2026-04-11 | 4.3 | CVE-2026-3371 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | reassign lessons between topics in any course, including admin-owned courses, by sending a crafted AJAX request with manipulated topic and lesson IDs. | | | |
| Thethinkery--Joomla iProperty Real Estate | Joomla iProperty Real Estate 4.1.1 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the filter_keyword parameter. Attackers can craft URLs containing JavaScript payloads in the filter_keyword GET parameter of the all-properties-with-map endpoint to execute arbitrary code in victim browsers and steal session tokens or credentials. | 2026-04-09 | 6.1 | CVE-2023-54361 |
| trailofbits--rfc3161-client | rfc3161-client is a Python library implementing the Time-Stamp Protocol (TSP) described in RFC 3161. Prior to 1.0.6, an Authorization Bypass vulnerability in rfc3161-client's signature verification allows any attacker to impersonate a trusted TimeStamping Authority (TSA). By exploiting a logic flaw in how the library extracts the leaf certificate from an unordered PKCS#7 bag of certificates, an attacker can append a spoofed certificate matching the target common_name and Extended Key Usage (EKU) requirements. This tricks the library into verifying these authorization rules against the forged certificate while validating the cryptographic signature against an actual trusted TSA (such as FreeTSA), thereby bypassing the intended TSA authorization pinning entirely. This vulnerability is fixed in 1.0.6. | 2026-04-08 | 6.2 | CVE-2026-33753 |
| uniquecodergmailcom--Pinterest Site Verification plugin using Meta Tag | The Pinterest Site Verification plugin using Meta Tag plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'post_var' parameter in versions up to, and including, 1.8 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. | 2026-04-08 | 6.4 | CVE-2026-3142 |
| usystemsgmbh--Webling | The Webling plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 3.9.0 due to insufficient input sanitization, insufficient output escaping, and missing capabilities checks in the 'webling_admin_save_form' and 'webling_admin_save_memberlist' functions. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject Webling forms and memberlists with arbitrary web scripts that will execute whenever an administrator views the related form or memberlist area of the WordPress admin. | 2026-04-10 | 6.4 | CVE-2026-1263 |
| Virtuemart--Cart | Joomla VirtueMart Shopping-Cart 4.0.12 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the keyword parameter. Attackers can craft malicious URLs containing script payloads in the keyword parameter of the product-variants endpoint to execute arbitrary JavaScript in victim browsers and steal session tokens or credentials. | 2026-04-09 | 6.1 | CVE-2023-54362 |
| vllm-project--vllm | vLLM is an inference and serving engine for large language models (LLMs). From 0.7.0 to before 0.19.0, the VideoMediaIO.load_base64() method at vllm/multimodal/media/video.py splits video/jpeg data URLs by comma to extract individual JPEG frames, but does not enforce a frame count limit. The num_frames parameter (default: 32), which is enforced by the load_bytes() code path, is completely bypassed in the video/jpeg base64 path. An attacker can send a single API request containing thousands of comma-separated base64-encoded JPEG frames, causing the server to decode all frames into memory and crash with OOM. This vulnerability is fixed in 0.19.0. | 2026-04-06 | 6.5 | CVE-2026-34755 |
| vllm-project--vllm | vLLM is an inference and serving engine for large language models (LLMs). From 0.1.0 to before 0.19.0, a Denial of Service vulnerability exists in the vLLM OpenAI-compatible API server. Due to the lack of an upper bound validation on the n parameter in the ChatCompletionRequest and CompletionRequest Pydantic models, an unauthenticated attacker can send a single HTTP request with an astronomically large n value. This completely blocks the Python asyncio event loop and causes immediate Out-Of-Memory crashes by allocating millions of request object copies in the heap before the request even reaches the scheduling queue. This vulnerability is fixed in 0.19.0. | 2026-04-06 | 6.5 | CVE-2026-34756 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| vllm-project--vllm | vLLM is an inference and serving engine for large language models (LLMs). From 0.16.0 to before 0.19.0, a server-side request forgery (SSRF) vulnerability in download_bytes_from_url allows any actor who can control batch input JSON to make the vLLM batch runner issue arbitrary HTTP/HTTPS requests from the server, without any URL validation or domain restrictions. This can be used to target internal services (e.g. cloud metadata endpoints or internal HTTP APIs) reachable from the vLLM host. This vulnerability is fixed in 0.19.0. | 2026-04-06 | 5.4 | CVE-2026-34753 |
| Volcengine--OpenViking | OpenViking versions prior to 0.3.3 contain a missing authorization vulnerability in the task polling endpoints that allows unauthorized attackers to enumerate or retrieve background task metadata created by other users. Attackers can access the /api/v1/tasks and /api/v1/tasks/{task_id} routes without authentication to expose task type, task status, resource identifiers, archive URIs, result payloads, and error information, potentially causing cross-tenant interference in multi-tenant deployments. | 2026-04-07 | 5.3 | CVE-2026-22680 |
| vsourz1td--Advanced Contact form 7 DB | The Advanced Contact form 7 DB plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.9. This is due to missing or incorrect nonce validation on the 'vsz_cf7_save_setting_callback' function. This makes it possible for unauthenticated attackers to delete form entry via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 2026-04-08 | 5.4 | CVE-2026-0811 |
| vsourz1td--Advanced Contact form 7 DB | The Advanced Contact form 7 DB plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'vsz_cf7_export_to_excel' function in all versions up to, and including, 2.0.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to export form submissions to excel file. | 2026-04-08 | 4.3 | CVE-2026-0814 |
| wpchill--Strong Testimonials | The Strong Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's testimonial_view shortcode in all versions up to, and including, 3.2.21 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 2026-04-08 | 6.4 | CVE-2026-3239 |
| wpeverest--User Registration & Membership Free & Paid Memberships, Subscriptions, Content Restriction, User Profile, Custom User Registration & Login Builder | The User Registration & Membership - Free & Paid Memberships, Subscriptions, Content Restriction, User Profile, Custom User Registration & Login Builder plugin for WordPress is vulnerable to SQL Injection via the 'membership_ids[]' parameter in all versions up to, and including, 5.1.2 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 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. | 2026-04-08 | 6.5 | CVE-2026-1865 |
| wpmudev--Hustle Email Marketing, Lead Generation, Optins, Popups | The Hustle - Email Marketing, Lead Generation, Optins, Popups plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'hustle_module_converted' AJAX action in all versions up to, and including, 7.8.10.2. This makes it possible for unauthenticated attackers to forge conversion tracking events for any Hustle module, including draft modules that are never displayed to users, thereby manipulating marketing analytics and conversion statistics. | 2026-04-07 | 5.3 | CVE-2026-2263 |
| ABB--AC800M (System 800xA) | A vulnerability exists in the command handling of the IEC 61850 communication stack included in the product revisions listed as affected in this CVE. An attacker with access to IEC 61850 networks could exploit the vulnera bility by using a specially crafted 61850 packet, forcing the communication interfaces of the PM 877, CI850 and CI868 modules into fault mode or causing unavailability of the S+ | 2026-04-13 | 6.5 | CVE-2025-3756 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | Operations 61850 connectivity, resulting in a denial-of-service situation. The System 800xA IEC61850 Connect is not affected. Note: This vulnerability does not impact on the overall availability and functionality of the S+ Operations node, only the 61850 communication function. This issue affects AC800M (System 800xA): from 6.0.0x through 6.0.0303.0, from 6.1.0x through 6.1.0031.0, from 6.1.1x through 6.1.1004.0, from 6.1.1x through 6.1.1202.0, from 6.2.0x through 6.2.0006.0; Symphony Plus SD Series: A_0, A_1, A_2.003, A_3.005, A_4.001, B_0.005; Symphony Plus MR (Melody Rack): from 3.10 through 3.52; S+ Operations: 2.1, 2.2, 2.3, 3.3. | | | |
| Adobe--Adobe Connect | Adobe Connect versions 2025.3, 12.10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Scope is changed. | 2026-04-14 | 6.1 | CVE-2026-21331 |
| cartasi--Nexi XPay | The Nexi XPay plugin for WordPress is vulnerable to unauthorized modification of data due to missing authorization checks on the redirect function in all versions up to, and including, 8.3.0. This makes it possible for unauthenticated attackers to mark pending WooCommerce orders as paid/completed. | 2026-04-14 | 5.3 | CVE-2025-15565 |
| Cisco--Cisco Identity Services Engine Software | A vulnerability in the CLI of Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC) could allow an authenticated, local attacker with administrative privileges to perform a command injection attack on the underlying operating system and elevate privileges to root. This vulnerability is due to insufficient validation of user supplied input. An attacker could exploit this vulnerability by providing crafted input to a specific CLI command. A successful exploit could allow the attacker to elevate their privileges to root on the underlying operating system. | 2026-04-15 | 6 | CVE-2026-20136 |
| Cisco--Cisco Identity Services Engine Software | Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker with administrative write privileges to conduct a stored cross-site scripting (XSS) attack or a reflected XSS attack against a user of the web-based management interface of an affected device. These vulnerabilities are due to insufficient sanitization of user-supplied data that is stored in the web page. An attacker could exploit these vulnerabilities by convincing a user of the interface to click a specific link or view an affected web page. The injected script code may be executed in the context of the web-based management interface or allow the attacker to access sensitive browser-based information. | 2026-04-15 | 4.8 | CVE-2026-20132 |
| Cisco--Cisco Identity Services Engine Software | A vulnerability in Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to perform path traversal attacks on the underlying operating system and read arbitrary files. To exploit this vulnerability, the attacker must have valid administrative credentials. 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 on the affected system. | 2026-04-15 | 4.9 | CVE-2026-20148 |
| Cisco--Cisco Secure Web Appliance | A vulnerability in the authentication service feature of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass authentication policy requirements. This vulnerability is due to improper validation of user-supplied authentication input in HTTP requests. An attacker could exploit this vulnerability by sending HTTP requests that contain specific authentication requests to an affected device. A successful exploit could allow the attacker to bypass policy enforcement on the device. There is no direct impact to the Cisco Secure Web Appliance. However, as a result of exploiting this vulnerability, an attacker could send HTTP requests that should be restricted through the device. | 2026-04-15 | 5.3 | CVE-2026-20152 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Cisco--Cisco ThousandEyes Enterprise Agent | A vulnerability in the CLI of Cisco ThousandEyes Enterprise Agent could allow an authenticated, local attacker with low privileges to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are on the local file system of an affected device. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system. A successful exploit could allow the attacker to bypass file system permissions and overwrite arbitrary files on the affected device. | 2026-04-15 | 5.5 | CVE-2026-20161 |
| Cisco--Cisco Unity Connection | A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a reflected XSS attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. | 2026-04-15 | 6.1 | CVE-2026-20059 |
| Cisco--Cisco Unity Connection | Multiple vulnerabilities in Cisco Unity Connection could allow an authenticated, remote attacker to download arbitrary files from an affected system. To exploit these vulnerabilities, the attacker must have valid administrative credentials.  These vulnerabilities are due to improper sanitization of user input to the web-based management interface. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request. A successful exploit could allow the attacker to download arbitrary files from an affected system. | 2026-04-15 | 6.5 | CVE-2026-20078 |
| Cisco--Cisco Unity Connection | Multiple vulnerabilities in Cisco Unity Connection could allow an authenticated, remote attacker to download arbitrary files from an affected system. To exploit these vulnerabilities, the attacker must have valid administrative credentials.  These vulnerabilities are due to improper sanitization of user input to the web-based management interface. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request. A successful exploit could allow the attacker to download arbitrary files from an affected system. | 2026-04-15 | 6.5 | CVE-2026-20081 |
| Cisco--Cisco Unity Connection | A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of HTTP request parameters. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious web page. | 2026-04-15 | 4.7 | CVE-2026-20060 |
| Cisco--Cisco Unity Connection | A vulnerability in the web-based management interface of Cisco Unity Connection could allow an authenticated, remote attacker to perform an SQL injection attack against an affected device. To exploit this vulnerability, the attacker must have valid user credentials on the affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP(S) request to the web-based management interface of an affected device. A successful exploit could allow the attacker to view data on the affected device. | 2026-04-15 | 4.3 | CVE-2026-20061 |
| Cisco--Cisco Webex Contact Center | A vulnerability in the Desktop Agent functionality of Cisco Webex Contact Center could have allowed an unauthenticated, remote attacker to conduct cross-site scripting attacks. Cisco has addressed this vulnerability in the Cisco Webex Contact Center service, and no customer action is needed. This vulnerability existed because HTML and script content was not properly handled. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by persuading a user to follow a malicious link. A successful exploit could have allowed the attacker to steal sensitive information from the browser, including authentication and session information. | 2026-04-15 | 6.1 | CVE-2026-20170 |
| Dell--Dell Pro 14 Essential PV14250 | Dell Client Platform BIOS contains a Weak Password Recovery Mechanism vulnerability. An unauthenticated attacker with physical access to the system could potentially exploit this vulnerability, leading to unauthorized access. | 2026-04-16 | 5.1 | CVE-2025-36579 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Dell--PowerProtect Data Domain | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain a session fixation vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. | 2026-04-17 | 6.2 | CVE-2025-46605 |
| Dell--PowerProtect Data Domain | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain an improper restriction of excessive authentication attempts vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. | 2026-04-17 | 6.2 | CVE-2025-46606 |
| Dell--PowerProtect Data Domain | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain an improper authentication vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. | 2026-04-17 | 6.6 | CVE-2025-46607 |
| Dell--PowerProtect Data Domain | Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain an improper authentication vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. | 2026-04-17 | 6.6 | CVE-2025-46641 |
| Dell--PowerScale OneFS | Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an insertion of sensitive information into log file vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account. | 2026-04-16 | 6.6 | CVE-2025-43937 |
| Dell--PowerScale OneFS | Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an improper check for unusual or exceptional conditions vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service. | 2026-04-16 | 4.1 | CVE-2025-43883 |
| Dell--PowerScale OneFS | Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an improper resource shutdown or release vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service. | 2026-04-16 | 4.4 | CVE-2025-43935 |
| DeluxeThemes--Userpro | Cross-Site Request Forgery (CSRF) vulnerability in DeluxeThemes Userpro allows Cross Site Request Forgery.This issue affects Userpro: from n/a before 5.1.11. | 2026-04-15 | 4.3 | CVE-2025-53444 |
| DesigningMedia--Eleganzo | The Eleganzo theme for WordPress is vulnerable to arbitrary directory deletion due to insufficient path validation in the akd_required_plugin_callback function in all versions up to, and including, 1.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary directories on the server, including the WordPress root directory. | 2026-04-14 | 6.5 | CVE-2025-15470 |
| Eaton--IPP Software | Due to improper input validation in one of the Eaton Intelligent Power Protector (IPP) XML, it is possible for an attacker with admin privileges and access to the local system to inject malicious code resulting in arbitrary command execution. This security issue has been fixed in the latest version of Eaton IPP software which is available on the Eaton download centre. | 2026-04-16 | 6 | CVE-2026-22615 |
| Eaton--IPP Software | Eaton Intelligent Power Protector (IPP) software allows repeated authentication attempts against the web interface login page due to insufficient rate-limiting controls. This security issue has been fixed in the latest version of Eaton IPP which is available on the Eaton download centre. | 2026-04-16 | 6.5 | CVE-2026-22616 |
| Eaton--IPP Software | Eaton Intelligent Power Protector (IPP) uses an insecure cookie configuration, which could allow a network-based attacker to intercept the cookie and exploit it through a man-in-the-middle attack. This security issue has been fixed in the latest version of Eaton IPP software which is available on the Eaton download centre. | 2026-04-16 | 5.7 | CVE-2026-22617 |
| Eaton--IPP software | A security misconfiguration was identified in Eaton Intelligent Power Protector (IPP), where an HTTP response header was set with an insecure attribute, potentially exposing users to web-based attacks. This security issue has been fixed | 2026-04-16 | 5.9 | CVE-2026-22618 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | in the latest version of Eaton IPP software which is available on the Eaton download centre. | | | |
| Emarket-design--YouTube Showcase | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Emarket-design YouTube Showcase allows Stored XSS.This issue affects YouTube Showcase: from n/a through 3.5.1. | 2026-04-15 | 6.5 | CVE-2025-15636 |
| flippercode--WP Maps Store Locator,Google Maps,OpenStreet Map,Mapbox,Listing,Directory & Filters | The WP Maps - Store Locator,Google Maps,OpenStreetMap,Mapbox,Listing,Directory & Filters plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'put_wpgm' shortcode in all versions up to, and including, 4.8.7. This is due to insufficient input sanitization and output escaping on user-supplied shortcode 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. | 2026-04-16 | 6.4 | CVE-2025-13364 |
| Fortinet--FortiManager | An improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.4, FortiAnalyzer 7.4.0 through 7.4.8, FortiAnalyzer 7.2 all versions, FortiAnalyzer 7.0 all versions, FortiAnalyzer Cloud 7.6.0 through 7.6.4, FortiAnalyzer Cloud 7.4.0 through 7.4.8, FortiAnalyzer Cloud 7.2 all versions, FortiAnalyzer Cloud 7.0 all versions, FortiManager 7.6.0 through 7.6.4, FortiManager 7.4.0 through 7.4.8, FortiManager 7.2 all versions, FortiManager 7.0 all versions, FortiManager Cloud 7.6.0 through 7.6.4, FortiManager Cloud 7.4.0 through 7.4.8, FortiManager Cloud 7.2 all versions, FortiManager Cloud 7.0 all versions may allow a privileged authenticated attacker to execute unauthorized code or commands via JSON RPC API | 2026-04-14 | 6.8 | CVE-2025-61848 |
| Fortinet--FortiManager Cloud | An improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.4, FortiAnalyzer 7.4.0 through 7.4.7, FortiAnalyzer 7.2 all versions, FortiAnalyzer 7.0 all versions, FortiAnalyzer Cloud 7.6.0 through 7.6.4, FortiAnalyzer Cloud 7.4.0 through 7.4.7, FortiAnalyzer Cloud 7.2 all versions, FortiAnalyzer Cloud 7.0 all versions, FortiManager 7.6.0 through 7.6.4, FortiManager 7.4.0 through 7.4.7, FortiManager 7.2 all versions, FortiManager 7.0 all versions, FortiManager Cloud 7.6.0 through 7.6.4, FortiManager Cloud 7.4.0 through 7.4.7, FortiManager Cloud 7.2 all versions, FortiManager Cloud 7.0 all versions may allow a privileged attacker to delete files from the underlying filesystem via crafted CLI requests. | 2026-04-14 | 5.4 | CVE-2025-68649 |
| Fortinet--FortiOS | A missing authentication for critical function vulnerability in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2.0 through 7.2.11, FortiOS 7.0.0 through 7.0.17, FortiOS 6.4 all versions, FortiOS 6.2.9 through 6.2.17 allows attacker to execute unauthorized code or commands via specially crafted packets. | 2026-04-14 | 6.2 | CVE-2025-53847 |
| Fortinet--FortiOS | An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') [CWE-22] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.4, FortiOS 7.4.0 through 7.4.9, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions, FortiPAM 1.7.0, 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 7.6.4, FortiProxy 7.4.0 through 7.4.11, FortiProxy 7.2 all versions, FortiProxy 7.0 all versions, FortiSwitchManager 7.2.0 through 7.2.7, FortiSwitchManager 7.0.0 through 7.0.6 may allow an authenticated attacker with admin profile and at least read-write permissions to write or delete arbitrary files via specific CLI commands. | 2026-04-14 | 5.4 | CVE-2025-61624 |
| Fortinet--FortiSandbox PaaS | An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability [CWE-79] vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.4, FortiSandbox PaaS 5.0.0 through 5.0.4 may allow an attacker to perform an XSS attack via crafted HTTP requests. | 2026-04-14 | 4.9 | CVE-2025-61886 |
| Fortinet--FortiSOAR on-premise | A cleartext transmission of sensitive information vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.3, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through | 2026-04-14 | 6.2 | CVE-2026-22155 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | 7.6.2, FortiSOAR on-premise 7.5.0 through 7.5.1, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow attacker to information disclosure via <insert attack vector here> | | | |
| Fortinet--FortiSOAR on-premise | An improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.3, FortiSOAR PaaS 7.5 all versions, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.3, FortiSOAR on-premise 7.5 all versions, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated remote attacker to perform path traversal attack via File Content Extraction actions. | 2026-04-14 | 6.2 | CVE-2026-22573 |
| Fortinet--FortiSOAR on-premise | A server-side request forgery (ssrf) vulnerability [CWE-918] vulnerability in Fortinet FortiSOAR PaaS 7.6.4, FortiSOAR PaaS 7.6.0 through 7.6.2, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.4, FortiSOAR on-premise 7.6.0 through 7.6.2, FortiSOAR on-premise 7.5.0 through 7.5.2, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated attacker to discover services running on local ports via crafted requests. | 2026-04-14 | 4.1 | CVE-2025-59809 |
| Fortinet--FortiSOAR PaaS | A cleartext transmission of sensitive information vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.3, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.2, FortiSOAR on-premise 7.5.0 through 7.5.1, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated attacker to view cleartext password in response for Secure Message Exchange and Radius queries, if configured | 2026-04-14 | 5.4 | CVE-2026-21742 |
| Fortinet--FortiSOAR PaaS | An improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.3, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.3, FortiSOAR on-premise 7.5.0 through 7.5.2, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated remote attacker to perform a stored cross site scripting (XSS) attack via crafted HTTP Requests. | 2026-04-14 | 4.4 | CVE-2026-22154 |
| Fortinet--FortiSOAR PaaS | A storing passwords in a recoverable format vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.4, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.4, FortiSOAR on-premise 7.5.0 through 7.5.2, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated remote attacker to retrieve Service account password via server address modification in LDAP configuration. | 2026-04-14 | 4.1 | CVE-2026-22574 |
| Fortinet--FortiSOAR PaaS | A storing passwords in a recoverable format vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.4, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.4, FortiSOAR on-premise 7.5.0 through 7.5.2, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated remote attacker to retrieve passwords for multiple installed connectors via server address modification in connector configuration. | 2026-04-14 | 4.1 | CVE-2026-22576 |
| Fortinet--FortiVoice | An exposure of sensitive information to an unauthorized actor vulnerability in Fortinet FortiNDR 7.6.0, FortiNDR 7.4.0 through 7.4.8, FortiNDR 7.2 all versions, FortiNDR 7.1 all versions, FortiNDR 7.0 all versions, FortiVoice 7.0.0 through 7.0.1 may allow a remote authenticated attacker with at least read-only permission on system maintenance to access backup information via crafted HTTP requests | 2026-04-14 | 5.4 | CVE-2024-23104 |
| Grafana--Loki | The CVE-2021-36156 fix validates the namespace parameter for path traversal sequences after a single URL decode, by double encoding, an attacker can read | 2026-04-15 | 5.3 | CVE-2026-21726 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | files at the Ruler API endpoint /loki/api/v1/rules/{namespace} Thanks to Prasanth Sundararajan for reporting this vulnerability. | | | |
| HCLSoftware--Velocity | Rate Limiting for attempting a user login is not being properly enforced, making HCL DevOps Velocity susceptible to brute-force attacks past the unsuccessful login attempt limit. This vulnerability is fixed in 5.1.7. | 2026-04-13 | 6.8 | CVE-2025-31991 |
| iberezansky--3D FlipBook PDF Embedder, PDF Flipbook Viewer, Flipbook Image Gallery | The 3D FlipBook - PDF Embedder, PDF Flipbook Viewer, Flipbook Image Gallery plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the send_post_pages_json() function in all versions up to, and including, 1.16.17. This makes it possible for unauthenticated attackers to retrieve flipbook page metadata for draft, private and password-protected flipbooks. | 2026-04-14 | 5.3 | CVE-2026-1314 |
| leaflet[.]com--Leaflet 1.9.4 | Leaflet versions up to and including 1.9.4 are vulnerable to Cross-Site Scripting (XSS) via the bindPopup() method. This method renders user-supplied input as raw HTML without sanitization, allowing attackers to inject arbitrary JavaScript code through event handler attributes (e.g., <img src=x onerror="alert('XSS')">). When a victim views an affected map popup, the malicious script executes in the context of the victim's browser session. | 2026-04-14 | 6.1 | CVE-2025-69993 |
| Lenovo--Service Bridge | A potential DLL hijacking vulnerability was reported in Lenovo Service Bridge that, under certain conditions, could allow a local authenticated user to execute code with elevated privileges. | 2026-04-15 | 6.7 | CVE-2026-1636 |
| livemesh--Livemesh Addons by Elementor | The Livemesh Addons for Elementor plugin for WordPress is vulnerable to unauthorized modification of data and Stored Cross-Site Scripting via plugin settings in all versions up to, and including, 9.0. This is due to missing authorization checks on the AJAX handler `lae_admin_ajax()` and insufficient output escaping on multiple checkbox settings fields. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in the plugin settings page that will execute whenever an administrator accesses the plugin settings page granted they can obtain a valid nonce, which can be leaked via the plugin's improper access control on settings pages. | 2026-04-16 | 6.4 | CVE-2026-1572 |
| Microsoft--Microsoft SharePoint Enterprise Server 2016 | Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network. | 2026-04-14 | 4.6 | CVE-2026-20945 |
| Microsoft--Windows 10 Version 1607 | Reliance on untrusted inputs in a security decision in Windows Boot Loader allows an authorized attacker to bypass a security feature locally. | 2026-04-14 | 6.7 | CVE-2026-0390 |
| Microsoft--Windows 10 Version 1607 | Improper removal of sensitive information before storage or transfer in Windows Recovery Environment Agent allows an unauthorized attacker to bypass a security feature with a physical attack. | 2026-04-14 | 4.6 | CVE-2026-20928 |
| Microsoft--Windows 10 Version 1809 | Access of resource using incompatible type ('type confusion') in Windows COM allows an authorized attacker to disclose information locally. | 2026-04-14 | 5.5 | CVE-2026-20806 |
| octobercms--october | October is a Content Management System (CMS) and web platform. Versions prior to 3.7.13 and versions 4.0.0 through 4.1.4 contain a sandbox bypass vulnerability in the optional Twig safe mode feature (CMS_SAFE_MODE). Certain methods on the collect() helper were not properly restricted, allowing authenticated users with template editing permissions to bypass sandbox protections. Exploitation requires authenticated backend access with CMS template editing permissions and only affects installations with CMS_SAFE_MODE enabled (disabled by default). This issue has been fixed in versions 3.7.13 and 4.1.5. To workaround this issue, users | 2026-04-14 | 4.9 | CVE-2026-22692 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | can disable CMS_SAFE_MODE if untrusted template editing is not required, and restrict CMS template editing permissions to fully trusted administrators only. | | | |
| prasunsen--Hostel | The Hostel plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'shortcode_id' parameter in all versions up to, and including, 1.1.6 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. | 2026-04-18 | 6.1 | CVE-2026-1838 |
| Samsung Mobile--Samsung Mobile Devices | Improper input validation in Retail Mode prior to SMR Apr-2026 Release 1 allows local attackers to trigger privileged functions. | 2026-04-13 | 6.6 | CVE-2026-21010 |
| SAP_SE--SAP Supplier Relationship Management (SICF Handler in SRM Catalog) | Due to a Cross-Site Scripting (XSS) vulnerability in the SAP Supplier Relationship Management (SICF Handler in SRM Catalog), an unauthenticated attacker could craft a malicious URL, that if accessed by a victim, results in execution of malicious content within the victim's browser. This could allow the attacker to access and modify information, impacting the confidentiality and integrity of the application, while availability remains unaffected. | 2026-04-14 | 6.1 | CVE-2026-0512 |
| Splunk--Splunk Enterprise | In Splunk Enterprise versions below 10.2.2, 10.0.5, 9.4.10, and 9.3.11, and Splunk Cloud Platform versions below 10.4.2603.0, 10.3.2512.6, 10.2.2510.10, 10.1.2507.20, 10.0.2503.13, and 9.3.2411.127, a user who holds a role that contains the high-privilege capability `edit_user`could create a specially crafted username that includes a null byte or a non-UTF-8 percent-encoded byte due to improper input validation.<br><br>This could lead to inconsistent conversion of usernames into a proper format for storage and account management inconsistencies, such as being unable to edit or delete affected users. | 2026-04-15 | 6.6 | CVE-2026-20202 |
| Splunk--Splunk Enterprise | In Splunk Enterprise versions below 10.2.2, 10.0.5, 9.4.10, and 9.3.11, and Splunk Cloud Platform versions below 10.4.2603.0, 10.3.2512.6, 10.2.2510.10, 10.1.2507.19, 10.0.2503.13, and 9.3.2411.127, a low-privileged user that does not hold the `admin` or `power` Splunk roles, has write permission on the app, and does not hold the high-privilege capability `accelerate_datamodel`, could turn on or off Data Model Acceleration due to improper access control. | 2026-04-15 | 4.3 | CVE-2026-20203 |
| surbma--Surbma \| Booking.com Shortcode | The Surbma \| Booking.com Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `surbma-bookingcom` shortcode in all versions up to, and including, 2.1 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. | 2026-04-14 | 6.4 | CVE-2026-1607 |
| themefusion--Avada (Fusion) Builder | The Avada (Fusion) Builder plugin for WordPress is vulnerable to Arbitrary WordPress Action Execution in all versions up to, and including, 3.15.1. This is due to the plugin's `output_action_hook()` function accepting user-controlled input to trigger any registered WordPress action hook without proper authorization checks. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary WordPress action hooks via the Dynamic Data feature, potentially leading to privilege escalation, file inclusion, denial of service, or other security impacts depending on which action hooks are available in the WordPress installation. | 2026-04-15 | 5.4 | CVE-2026-1509 |
| themefusion--Avada (Fusion) Builder | The Avada (Fusion) Builder plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.15.1. This is due to the plugin's `fusion_get_post_custom_field()` function failing to validate whether metadata keys are protected (underscore-prefixed). This makes it possible for authenticated attackers, with Subscriber-level access and above, to extract protected post metadata fields that should not be publicly accessible via the Dynamic Data feature's `post_custom_field` parameter. | 2026-04-15 | 4.3 | CVE-2026-1541 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| turn2honey--EMC Easily Embed Calendly Scheduling | The EMC - Easily Embed Calendly Scheduling Features plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's calendly shortcode in all versions up to, and including, 4.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 2026-04-19 | 6.4 | CVE-2026-0868 |
| vanderwijk--Content Blocks (Custom Post Widget) | The Content Blocks (Custom Post Widget) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's content_block shortcode in all versions up to, and including, 3.3.9 due to insufficient input sanitization and output escaping on user supplied values consumed from user-created content blocks. 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. | 2026-04-18 | 6.4 | CVE-2026-0894 |
| Vision--Helpdesk | Vision Helpdesk before 5.7.0 (patched in 5.6.10) allows attackers to read user profiles via modified serialized cookie data to vis_client_id. | 2026-04-16 | 4.3 | CVE-2024-58343 |
| Wago--Smart Designer | In Wago Smart Designer in versions up to 2.33.1 a low privileged remote attacker may enumerate projects and usernames through iterative requests to an specific endpoint. | 2026-04-16 | 4.3 | CVE-2023-5872 |
| woobeewoo--Product Pricing Table by WooBeWoo | The Product Pricing Table by WooBeWoo plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.0. This is due to missing or incorrect nonce validation on the updateLabel() and remove() functions. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages or delete pricing tables via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | 2026-04-15 | 6.1 | CVE-2026-1852 |
| Wpmet--MetForm Pro | The MetForm Pro plugin for WordPress is vulnerable to Improper Input Validation in all versions up to, and including, 3.9.7 This is due to the payment integrations (Stripe/PayPal) trusting a user-submitted calculation field value without recomputing or validating it against the configured form price. This makes it possible for unauthenticated attackers to manipulate the payment amount via the 'mf-calculation' field in the form submission REST request granted there exists a specific form with this particular configuration. | 2026-04-15 | 5.3 | CVE-2026-1782 |
| wpxpo--Post Grid Gutenberg Blocks for News, Magazines, Blog Websites PostX | The Post Grid Gutenberg Blocks for News, Magazines, Blog Websites - PostX plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ultp_shareCount_callback() function in all versions up to, and including, 5.0.5. This makes it possible for unauthenticated attackers to modify the share_count post meta for any post, including private or draft posts. | 2026-04-16 | 5.3 | CVE-2026-0718 |
| WSO2--WSO2 API Manager | The authentication endpoint fails to adequately validate user-supplied input before reflecting it back in the response. This allows an attacker to inject malicious script payloads into the input parameters, which are then executed by the victim's browser. Successful exploitation can enable an attacker to redirect the user's browser to a malicious website, modify the UI of the web page, or retrieve information from the browser. However, the impact is limited as session-related sensitive cookies are protected by the httpOnly flag, preventing session hijacking. | 2026-04-16 | 6.1 | CVE-2024-10242 |
| WSO2--WSO2 API Manager | The authentication endpoint fails to encode user-supplied input before rendering it in the web page, allowing for script injection. An attacker can leverage this by injecting malicious scripts into the authentication endpoint. This can result in the user's browser being redirected to a malicious website, manipulation of the web page's user interface, or the retrieval of information from the browser. However, session hijacking is not possible due to the httpOnly flag protecting session-related cookies. | 2026-04-16 | 6.1 | CVE-2025-6024 |
| WSO2--WSO2 API Manager | The WSO2 API Manager developer portal accepts user-supplied input without enforcing expected validation constraints or proper output encoding. This deficiency allows a malicious actor to inject script content that is executed within | 2026-04-16 | 5.4 | CVE-2024-4867 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | the context of a user's browser. By leveraging this cross-site scripting vulnerability, a malicious actor can cause the browser to redirect to a malicious website, make changes to the UI of the web page, or retrieve information from the browser. However, session hijacking is not possible as all session-related sensitive cookies are protected by the httpOnly flag. | | | |
| WSO2--WSO2 Identity Server | Active access tokens are not revoked or invalidated when a user account is locked within WSO2 Identity Server. This failure to enforce revocation allows previously issued, valid tokens to remain usable, enabling continued access to protected resources by locked user accounts. The security consequence is that a locked user account can maintain access to protected resources through the use of existing, unexpired access tokens. This creates a security gap where access control policies are bypassed, potentially leading to unauthorized data access or actions until the tokens naturally expire. | 2026-04-16 | 6 | CVE-2025-12624 |
| youzify--Youzify BuddyPress Community, User Profile, Social Network & Membership Plugin for WordPress | The Youzify plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'checkin_place_id' parameter in all versions up to, and including, 1.3.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | 2026-04-18 | 6.4 | CVE-2026-1559 |
| Zaytech--Smart Online Order for Clover | Cross-Site Request Forgery (CSRF) vulnerability in Zaytech Smart Online Order for Clover allows Cross Site Request Forgery.This issue affects Smart Online Order for Clover: from n/a through 1.6.0. | 2026-04-15 | 4.3 | CVE-2025-15635 |
| 94Cb--Carbon Forum | Carbon Forum 5.9.0 contains a persistent cross-site scripting vulnerability that allows authenticated administrators to inject malicious JavaScript code through the Forum Name field in dashboard settings. Attackers with admin privileges can store JavaScript payloads in the Forum Name field that execute in the browsers of all users visiting the forum, enabling session hijacking and data theft. | 2026-04-22 | 6.4 | CVE-2024-58344 |
| Acutesystems--CrossFont | CrossFont 7.5 contains a buffer overflow vulnerability that allows local attackers to crash the application by submitting an oversized payload in the License Key field. Attackers can generate a malicious file containing 4000 bytes of data, paste it into the License Key input field, and trigger an application crash when processing the input. | 2026-04-26 | 6.2 | CVE-2018-25273 |
| Acutesystems--TransMac | TransMac 12.2 contains a buffer overflow vulnerability in the license key input field that allows local attackers to crash the application by submitting an oversized string. Attackers can generate a payload file containing 4000 bytes of data, paste it into the License Key field, and trigger a denial of service condition. | 2026-04-26 | 6.2 | CVE-2018-25264 |
| Angryip--Angry IP Scanner | Angry IP Scanner 3.5.3 contains a buffer overflow vulnerability in the preferences dialog that allows local attackers to crash the application by supplying an excessively large string. Attackers can generate a file containing a massive buffer of repeated characters and paste it into the unavailable value field in the display preferences to trigger a denial of service. | 2026-04-22 | 6.2 | CVE-2018-25266 |
| Angryip--Angry IP Scanner for Linux | Angry IP Scanner for Linux 3.5.3 contains a denial of service vulnerability that allows local attackers to crash the application by supplying malformed input to the port selection field. Attackers can craft a malicious string containing buffer overflow patterns and paste it into the Preferences Ports tab to trigger an application crash. | 2026-04-22 | 6.2 | CVE-2018-25262 |
| Bome--Restorator | Bome Restorator 1793 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Name field. Attackers can create a malicious payload exceeding 4000 bytes and | 2026-04-26 | 6.2 | CVE-2018-25292 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | paste it into the Name input field to trigger an application crash and denial of service. | | | |
| Br-Software--PixGPS | PixGPS 1.1.8 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an oversized string to the folder path input field. Attackers can craft a payload exceeding 6000 bytes and paste it into the 'Folder with picture files' field to trigger a denial of service condition. | 2026-04-26 | 6.2 | CVE-2018-25277 |
| Convertimagetotext--jiNa OCR Image to Text | jiNa OCR Image to Text 1.0 contains a denial of service vulnerability that allows local attackers to crash the application by processing a malformed PNG file. Attackers can create a specially crafted PNG file with an oversized buffer and trigger the crash when the application attempts to convert the file to PDF. | 2026-04-26 | 6.2 | CVE-2018-25279 |
| Editorsoftware--StyleWriter | StyleWriter 1.0 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long string. Attackers can paste a 6000-byte payload into the Pattern to Find or Advice Message fields in the Add Pattern dialog to trigger a denial of service condition. | 2026-04-26 | 6.2 | CVE-2018-25288 |
| Ezbsystems--Easyboot | Easyboot 6.6.0 contains a buffer overflow vulnerability in the Replace Text function that allows local attackers to crash the application by supplying an oversized string. Attackers can trigger the vulnerability by accessing File > Tools > Replace Text and pasting a 7000-byte payload into the text fields to cause a denial of service. | 2026-04-26 | 6.2 | CVE-2018-25290 |
| Ezbsystems--Softdisk | Softdisk 3.0.3 contains a buffer overflow vulnerability in the registration code dialog that allows local attackers to crash the application by supplying an oversized string. Attackers can trigger the vulnerability by entering a 6000-byte payload in the Registration Name field through the Help menu's Enter Registration Code dialog to cause a denial of service. | 2026-04-26 | 6.2 | CVE-2018-25289 |
| faleemi--Faleemi Plus | Faleemi Plus 1.0.2 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying oversized input strings. Attackers can paste a 2000-byte payload into the Camera name and DID number fields during camera addition to trigger an application crash. | 2026-04-26 | 6.2 | CVE-2018-25275 |
| Fathom--Fathom | Fathom 2.4 contains a buffer overflow vulnerability in the Authorization Code field that allows local attackers to crash the application by submitting an oversized input string. Attackers can paste a 6000-byte payload into the Authorization Code field and click Activate to trigger a denial of service condition. | 2026-04-26 | 5.5 | CVE-2018-25285 |
| Fortra--GoAnywhere MFT | Encrypted values in Fortra's GoAnywhere MFT prior to version 7.10.0 and GoAnywhere Agents prior to version 2.2.0 utilize a static IV which allows admin users to brute-force decryption of data. | 2026-04-21 | 5.8 | CVE-2025-1241 |
| GitLab--GitLab | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 10.6 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1 that could have allowed an authenticated user to cause denial of service under certain conditions by exhausting server resources by making crafted requests to a discussions endpoint. | 2026-04-22 | 6.5 | CVE-2025-0186 |
| GitLab--GitLab | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.4 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1 that could have allowed an authenticated user to cause denial of service by overwhelming system resources under certain conditions due to insufficient resource allocation limits in the GraphQL API. | 2026-04-22 | 6.5 | CVE-2025-3922 |
| HCLSoftware--BigFix Service Management (SM) | HCL BigFix Service Management (SM) Discovery is vulnerable to unenforced encryption due to port 80 (HTTP) being open, allowing unencrypted access. An attacker with access to the network traffic can sniff packets from the connection and uncover the data. | 2026-04-21 | 5.3 | CVE-2025-31981 |
| Hdtune--Drive Power Manager | Drive Power Manager 1.10 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long string in the | 2026-04-26 | 5.5 | CVE-2018-25287 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | Name field. Attackers can paste a 6000-byte payload into the Name field and click Register to trigger a denial of service condition. | | | |
| Hdtune--Easy PhotoResQ | Easy PhotoResQ 1.0 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long string in the Folder/filename field. Attackers can input a 6000-byte payload through the File Options dialog to trigger a denial of service condition. | 2026-04-26 | 6.2 | CVE-2018-25286 |
| Hdtune--HD Tune Pro | HD Tune Pro 5.70 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an excessively long string in the folder/file name field. Attackers can trigger a denial of service by entering a 6000-byte payload through the File > Options > Save dialog's folder/file name input field. | 2026-04-26 | 6.2 | CVE-2018-25284 |
| 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, 11.3.32 via the leadin/public/admin/class-adminconstants.php file. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract a list of all installed plugins and their versions which can be leveraged for reconnaissance and further attacks. | 2026-04-24 | 4.3 | CVE-2025-11762 |
| IBM--Security Verify Directory (Container) | IBM Security Verify Directory (Container) 10.0.0 through 10.0.0.3 IBM Security Verify Directory could be vulnerable to malicious file upload by not validating file type. A privileged user could upload malicious files into the system that can be sent to victims for performing further attacks against the system. | 2026-04-22 | 5.5 | CVE-2025-36074 |
| icewarp--ICEWARP Client | ICEWARP 11.0.0.0 contains a cross-site scripting vulnerability that allows attackers to inject malicious HTML elements into emails by embedding base64-encoded payloads in object and embed tags. Attackers can craft emails containing data URIs with embedded scripts that execute in the client when the email is viewed, compromising user sessions and stealing sensitive information. | 2026-04-22 | 6.1 | CVE-2018-25269 |
| Infiltration-Systems--Infiltrator Network Security Scanner | Infiltrator Network Security Scanner 4.6 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an oversized input string. Attackers can paste a 6000-byte payload into the Scan Target field and trigger a denial of service condition when the Scan button is clicked. | 2026-04-26 | 5.5 | CVE-2018-25280 |
| infrarecorder--InfraRecorder | InfraRecorder 0.53 contains a denial of service vulnerability that allows local attackers to crash the application by importing a maliciously crafted text file. Attackers can create a text file containing 6000 bytes of data and import it through the Edit menu's Import function to trigger an application crash. | 2026-04-26 | 6.2 | CVE-2018-25274 |
| Maxprog--iCash | iCash 7.6.5 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying an oversized payload through the Connect to Server dialog. Attackers can paste a 7000-byte string into the Host field and click Connect to trigger an application crash. | 2026-04-26 | 5.5 | CVE-2018-25281 |
| Mersenne--Prime95 | Prime95 29.4b7 contains a buffer overflow vulnerability in the PrimeNet connection dialog that allows local attackers to crash the application by supplying an excessively long string in the optional proxy password field. Attackers can trigger a denial of service by entering a 6000-byte payload into the proxy password parameter, causing the application to crash when processing the connection settings. | 2026-04-26 | 6.2 | CVE-2018-25293 |
| OpenSC--OpenSC | Multiple uses of uninitialized variables were found in libopensc that may lead to information disclosure or application crash. An attack requires a crafted USB device or smart card that would present the system with specially crafted responses to the APDUs | 2026-04-23 | 5.7 | CVE-2025-13763 |
| P10--Central Management Software | P10 Central Management Software 1.4.13 contains a buffer overflow vulnerability in the login password field that allows local attackers to crash the application by submitting an oversized input string. Attackers can paste a 2000-byte payload into | 2026-04-26 | 5.5 | CVE-2018-25296 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | the password field and click login to trigger an application crash and denial of service. | | | |
| P10--ObserverIP Scan Tool | ObserverIP Scan Tool 1.4.0.1 contains a denial of service vulnerability that allows local attackers to crash the application by submitting an excessively long string in the IP input field. Attackers can paste a 2000-byte buffer of repeated characters into the IP field and trigger a search operation to cause an application crash. | 2026-04-26 | 6.2 | CVE-2018-25295 |
| Picajet--PicaJet FX | PicaJet FX 2.6.5 contains a denial of service vulnerability that allows local attackers to crash the application by submitting oversized input to registration fields. Attackers can paste a 6000-byte buffer into the Registration Name and Registration Key fields via the Help menu's Register PicaJet dialog to trigger an application crash. | 2026-04-26 | 6.2 | CVE-2018-25278 |
| Picajet--RoboImport | RoboImport 1.2.0.72 contains a denial of service vulnerability that allows local attackers to crash the application by submitting oversized input to registration fields. Attackers can paste a 6000-byte buffer into the Registration Name and Registration Key fields and click Register to trigger an application crash. | 2026-04-26 | 5.5 | CVE-2018-25276 |
| Pj64-Emu--Project64 | Project64 2.3.2 contains a buffer overflow vulnerability in the Plugin Directory settings field that allows local attackers to crash the application by supplying an excessively long string. Attackers can input a 6000-byte payload into the Plugin Directory field through the Options > Settings > Directories interface to trigger an application crash when settings are reopened. | 2026-04-26 | 6.2 | CVE-2018-25291 |
| Textpad--Textpad | Textpad 8.1.2 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an excessively long buffer string through the Run command interface. Attackers can paste a 5000-byte payload into the Command field via Tools > Run to trigger a buffer overflow that crashes the application. | 2026-04-22 | 6.2 | CVE-2018-25271 |
| Ultraiso--UltraISO | UltraISO 9.7.1.3519 contains a local buffer overflow vulnerability in the Output FileName field of the Make CD/DVD Image dialog that allows attackers to overwrite SEH and SE handler records. Attackers can craft a malicious filename string with 304 bytes of data followed by SEH record overwrite values and paste it into the Output FileName field to trigger a denial of service crash. | 2026-04-22 | 6.2 | CVE-2018-25267 |
| Wansview--Wansview | Wansview 1.0.2 contains a buffer overflow vulnerability that allows local attackers to crash the application by supplying oversized input strings. Attackers can inject 2000-byte payloads into the Camera name and DID number fields during camera addition to trigger application crashes. | 2026-04-26 | 6.2 | CVE-2018-25297 |
| ZenMap--ZenMap | Nmap 7.70 contains a denial of service vulnerability that allows local attackers to crash the application by processing malicious XML files with exponential entity expansion. Attackers can create a crafted XML file with nested entity definitions and open it through ZenMap's scan import functionality to cause the program to consume excessive system resources and crash. | 2026-04-26 | 6.2 | CVE-2018-25282 |
| 8nite--metatrader-4-mcp | A security vulnerability has been detected in 8nite metatrader-4-mcp 1.0.0. This vulnerability affects the function CallToolRequestSchema of the file src/index.ts of the component sync_ea_from_file. Such manipulation of the argument ea_name leads to path traversal. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet. | 2026-05-02 | 6.3 | CVE-2026-7627 |
| Acrel Electrical--EEMS Enterprise Power Operation and Maintenance Cloud Platform | A vulnerability was found in Acrel Electrical EEMS Enterprise Power Operation and Maintenance Cloud Platform 1.3.0. This impacts an unknown function of the file /SubstationWEBV2/main/uploadH5Files. The manipulation of the argument File results in unrestricted upload. The attack may 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. | 2026-05-03 | 6.3 | CVE-2026-7696 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| AMTT--Hotel Broadband Operation System | A vulnerability was determined in AMTT Hotel Broadband Operation System 1.0. Affected is an unknown function of the file /manager/card/cardhand_submit.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. 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. | 2026-05-03 | 4.7 | CVE-2026-7697 |
| appcheap--App Builder Create Native Android & iOS Apps On The Flight | The App Builder - Create Native Android & iOS Apps On The Flight plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to and including 5.6.0. This is due to missing authorization validation in the `upload_avatar()` function, which accepts an attacker-controlled `user_id` parameter from the POST request body and uses it to update user meta without verifying that the authenticated requester owns or has permission to modify the target account. This makes it possible for authenticated attackers, with Subscriber-level access and above, to overwrite the profile avatar of any arbitrary user on the site, including administrators, by supplying a target `user_id` in the request body to the `/wp-json/app-builder/v1/upload-avatar` endpoint. | 2026-05-02 | 5.3 | CVE-2026-7638 |
| ArtMin96--yii2-mcp-server | A flaw has been found in ArtMin96 yii2-mcp-server 1.0.2. This impacts the function yii_command_help/yii_execute_command of the file src/index.ts of the component MCP Interface. Executing a manipulation can lead to os command injection. 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. | 2026-05-02 | 6.3 | CVE-2026-7600 |
| AV Stumpfl--Pixera Two Media Server | A vulnerability has been found in AV Stumpfl Pixera Two Media Server up to 25.1 R2. The affected element is an unknown function of the component Service Port 1338. Such manipulation leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 25.2 R3 is sufficient to fix this issue. It is advisable to upgrade the affected component. | 2026-05-03 | 4.3 | CVE-2026-7704 |
| chartbrew--chartbrew | Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. In version 4.9.0, the endpoint POST /user/invited does not validate any invite token, authentication header, or session. Any unauthenticated attacker can call this endpoint directly to create a fully active account and receive a valid JWT - even when the instance has existing users and signupRestricted is enabled. This bypass is distinct from the normal registration endpoint (POST /user) which enforces signupRestricted and sets active: false pending verification. This issue has been patched in version 5.0.0. | 2026-04-30 | 6.5 | CVE-2026-35514 |
| chartbrew--chartbrew | Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. In version 4.9.0, Chartbrew exposes a legacy dashboard route that returns a project's report data to any authenticated member of the same team, even when that user does not have access to the specific project. The route bypasses project-level authorization and returns the raw project object. As a result, a low-privileged same-team user can read another project's dashboard data and recover the project's stored report password from the response. This issue has been patched in version 5.0.0. | 2026-04-30 | 6.5 | CVE-2026-40603 |
| ChatGPTNextWeb--NextChat | A flaw has been found in ChatGPTNextWeb NextChat up to 2.16.1. This impacts an unknown function of the file Next.js of the component API Endpoint. Executing a manipulation can lead to permissive cross-domain policy with untrusted domains. The attack may 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. | 2026-05-02 | 4.3 | CVE-2026-7643 |
| code-projects--Online Hospital Management System | A vulnerability was found in code-projects Online Hospital Management System 1.0. The impacted element is an unknown function of the component Registration Handler. The manipulation of the argument Username results in improper authorization. The attack can be executed remotely. The exploit has been made public and could be used. | 2026-05-02 | 5.4 | CVE-2026-7631 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| complianz--Complianz GDPR/CCPA Cookie Consent | The Complianz - GDPR/CCPA Cookie Consent plugin for WordPress is vulnerable to unauthorized data access in all versions up to, and including, 7.4.5 This is due to the REST API endpoint at /wp-json/complianz/v1/consent-area/{post_id}/{block_id} using __return_true as the permission_callback, allowing any unauthenticated user to access it. The cmplz_rest_consented_content() function retrieves a post by ID via get_post() and returns the consentedContent attribute of any complianz/consent-area block found in it, without checking if the post is published or if the user has permission to read it. This makes it possible for unauthenticated attackers to read the consent area block content from private, draft, or unpublished posts. | 2026-04-29 | 5.3 | CVE-2026-4019 |
| crazyrabbitLTC--mcp-code-review-server | A vulnerability was detected in crazyrabbitLTC mcp-code-review-server up to 0.1.0. This issue affects the function executeRepomix of the file src/repomix.ts of the component RepoMix Command Handler. Performing a manipulation results in command injection. The attack may be initiated remotely. The exploit is now public and may be used. The project was informed of the problem early through a pull request but has not reacted yet. | 2026-05-02 | 6.3 | CVE-2026-7628 |
| Dayoooun--hwpx-mcp | A vulnerability was detected in Dayoooun hwpx-mcp 0.2.0. This affects the function save_document/export_to_text/export_to_html of the file mcp-server/src/index.ts of the component MCP Interface. Performing a manipulation of the argument output_path results in path traversal. 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. | 2026-05-01 | 6.3 | CVE-2026-7599 |
| Dell--Alienware Command Center (AWCC) | Dell Alienware Command Center (AWCC), versions prior to 6.13.8.0, contain an Execution with Unnecessary Privileges vulnerability in the AWCC. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges. | 2026-04-27 | 6.7 | CVE-2026-25908 |
| Dell--Alienware Command Center (AWCC) | Dell Alienware Command Center (AWCC), versions prior to 6.13.8.0, contain a Least Privilege Violation vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges. | 2026-04-27 | 5.3 | CVE-2026-32655 |
| Dell--Dell/Alienware Purchased Apps | Dell/Alienware Purchased Apps, versions prior to 1.1.31.0, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Arbitrary File Write | 2026-04-29 | 6.3 | CVE-2026-27105 |
| diplodoc-platform--@diplodoc/search-extension | @diplodoc/search-extension 1.0.0 through 3.x before 3.0.3 allows stored XSS via the title in a .md file. | 2026-05-01 | 5.4 | CVE-2026-40201 |
| dokaninc--Dokan: AI Powered WooCommerce Multivendor Marketplace Solution Build Your Own Amazon, eBay, Etsy | The Dokan: AI Powered WooCommerce Multivendor Marketplace Solution plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.3.1 via the '/dokan/v1/stores/{id}/reviews' REST API endpoint. This is due to the 'prepare_reviews_for_response' method including reviewer email addresses, usernames, and user IDs in the API response. This makes it possible for unauthenticated attackers to extract email addresses, usernames, and user IDs of all customers who left reviews on any vendor's store. The Pro version of the plugin must be installed and activated, with store reviews enabled, in order to exploit the vulnerability. | 2026-05-02 | 5.3 | CVE-2026-3504 |
| Dolibarr--ERP CRM | A vulnerability was identified in Dolibarr ERP CRM up to 23.0.2. This affects the function _checkValForAPI of the file htdocs/expedition/class/expedition.class.php of the component Shipments API Endpoint. The manipulation of the argument fields leads to sql injection. The attack is possible to be carried out remotely. A high degree of complexity is needed for the attack. It is indicated that the exploitability is difficult. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 5 | CVE-2026-7688 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Dromara--MaxKey | A security flaw has been discovered in Dromara MaxKey up to 3.5.13. Affected by this issue is the function StrUtils.checkSqlInjection of the file StrUtils.java. Performing a manipulation of the argument filtersfields results in sql 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 was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 6.3 | CVE-2026-7699 |
| Edimax--BR-6208AC | A security flaw has been discovered in Edimax BR-6208AC 1.02. The impacted element is the function setWAN of the file /goform/setWAN of the component L2TP Mode. The manipulation of the argument L2TPUserName results in command injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 6.3 | CVE-2026-7682 |
| Edimax--BR-6428nC | A weakness has been identified in Edimax BR-6428nC up to 1.16. This affects an unknown function of the file /goform/setWAN of the component Web Interface. This manipulation of the argument pppUserName/pptpUserName causes command injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 6.3 | CVE-2026-7683 |
| Elastic--Elastic Package Registry | Improper Verification of Cryptographic Signature (CWE-347) in Elastic Package Registry could allow an attacker positioned to intercept network traffic, or to otherwise influence the contents served to a self-hosted registry, to substitute a tampered package without the integrity check failing closed. | 2026-04-28 | 5.9 | CVE-2026-33467 |
| Exim--Exim | In Exim before 4.99.2, on systems using musl libc (not glibc), an attacker can crash the connection instance when malformed DNS data is present in PTR records. This is caused by a dn_expand oddity in octal printing. | 2026-04-30 | 5.9 | CVE-2026-40684 |
| eyeo--Adblock Plus | A vulnerability was found in eyeo Adblock Plus up to 4.36.2 on Chrome. Affected by this vulnerability is the function postMessage of the file premium.preload.js of the component Legacy Premium Activation. Performing a manipulation results in improper access controls. Remote exploitation of the attack is possible. The exploit has been made public and could be used. Upgrading the affected component is recommended. The vendor provides additional details: "The affected code path is a legacy Premium activation flow that has been deprecated. eyeo has already migrated to a new user account-based licensing system. The exploit does not grant permanent Premium access. The licensing server issues a short-lived trial license (valid for approximately 24 hours) for any submitted userId. On the next license check, the server validates against a real subscription and the trial expires if no valid subscription is found. The researcher's claim of permanently unlocking all Premium features is therefore incorrect. (...) The old flow has been present for years and has not been weaponized at scale to our knowledge. The risk to eyeo and to users is minimal." | 2026-05-03 | 5.3 | CVE-2026-7686 |
| gnu--wget2 | wget2 accepts a server certificate with incorrect Key Usage (KU) or Extended Key Usage (EKU). If the attackers compromise a certificate (with the associated private key) issued for a different purpose, they may be able to reuse it for TLS server authentication. | 2026-04-29 | 4.8 | CVE-2026-1858 |
| IBM--Db2 | IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.3 for Linux, UNIX and Windows (includes DB2 Connect Server) could allow an authenticated user to cause a denial of service using a specially crafted SQL query due to improper allocation of system resources. | 2026-04-30 | 6.5 | CVE-2025-36122 |
| IBM--Db2 | IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4 for Linux, UNIX and Windows (includes Db2 Connect Server) could allow an authenticated user to cause a denial of service due to improper neutralization of special elements in data query logic. | 2026-04-30 | 6.5 | CVE-2026-1577 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| IBM--Db2 | IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.3 for Linux, UNIX and Windows (includes Db2 Connect Server) could allow an authenticated user to cause a denial of service due to improper neutralization of special elements in data query logic when certain configurations exist. | 2026-04-30 | 5.3 | CVE-2025-14688 |
| IBM--Langflow Desktop | IBM Langflow Desktop 1.0.0 through 1.8.4 IBM Langflow is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. | 2026-04-30 | 6.5 | CVE-2026-3340 |
| IBM--Langflow Desktop | IBM Langflow Desktop <=1.8.4 Langflow 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. | 2026-04-30 | 6.5 | CVE-2026-3345 |
| IBM--Langflow Desktop | IBM Langflow Desktop 1.6.0 through 1.8.4 Lanflow is vulnerable to stored cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. | 2026-04-30 | 6.4 | CVE-2026-3346 |
| IBM--watsonx.data | IBM watsonx.data 2.2 through 2.3 IBM Lakehouse does not properly restrict communication between pods which could allow an attacker to transfer data between pods without restrictions. | 2026-04-30 | 5.3 | CVE-2025-36180 |
| IBM--watsonx.data intelligence | IBM watsonx.data intelligence 5.2.0, 5.2.1, 5.3.0, 5.3.1 stores user credentials in plain text which can be read by a local user. | 2026-04-30 | 6.2 | CVE-2025-36335 |
| itsourcecode--Courier Management System | A vulnerability was determined in itsourcecode Courier Management System 1.0. Affected is an unknown function of the file /edit_user.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. | 2026-05-02 | 4.7 | CVE-2026-7612 |
| janeczku--Calibre-Web | A vulnerability was identified in janeczku Calibre-Web up to 0.6.26. The impacted element is the function generate_auth_token of the file cps/kobo_auth.py of the component Endpoint. Such manipulation of the argument user_id leads to improper authorization. The attack may be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 6.3 | CVE-2026-7709 |
| JD Cloud--JDCOS | A flaw has been found in JD Cloud JDCOS 4.5.1.r4518. This vulnerability affects the function set_iptv_info of the file /jdcap of the component Service Interface. Executing a manipulation of the argument vid can lead to command injection. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 6.3 | CVE-2026-7705 |
| jsbroks--COCO Annotator | A security vulnerability has been detected in jsbroks COCO Annotator up to 0.11.1. Affected by this vulnerability is an unknown functionality of the file backend/webserver/api/datasets.py of the component Dataset API. The manipulation of the argument DatasetId leads to authorization bypass. 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. | 2026-05-03 | 6.5 | CVE-2026-7681 |
| jsbroks--COCO Annotator | A weakness has been identified in jsbroks COCO Annotator up to 0.11.1. Affected is an unknown function of the file backend/webserver/api/datasets.py of the component Data Endpoint. Executing a manipulation of the argument folder can lead to path traversal. 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. | 2026-05-03 | 4.3 | CVE-2026-7680 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| kerwincui--FastBee | A vulnerability was found in kerwincui FastBee up to 1.2.1. The affected element is the function ToolController.download of the file springboot/fastbee-open-api/src/main/java/com/fastbee/data/controller/ToolController.java of the component Tool Download Endpoint. The manipulation of the argument fileName results in path traversal. 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. | 2026-05-03 | 4.3 | CVE-2026-7676 |
| kleneway--awesome-cursor-mpc-server | A flaw has been found in kleneway awesome-cursor-mpc-server up to 2.0.1. Impacted is the function runCodeReviewTool of the file src/tools/codeReview.ts of the component Ccode-Review Tool. Executing a manipulation can lead to command injection. The attack may be launched remotely. The exploit has been published and may be used. The project was informed of the problem early through a pull request but has not reacted yet. | 2026-05-02 | 6.3 | CVE-2026-7629 |
| langflow-ai--langflow | A vulnerability was determined in langflow-ai langflow up to 1.8.4. Affected by this issue is the function CodeParser.parse_callable_details of the file src/lfx/src/lfx/custom/code_parser/code_parser.py of the component Full Builtins Module Handler. Executing a manipulation can lead to command injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 6.3 | CVE-2026-7687 |
| langflow-ai--langflow | A weakness has been identified in langflow-ai langflow up to 1.8.4. This affects the function eval of the file src/lfx/src/lfx/components/llm_operations/lambda_filter.p of the component LambdaFilterComponent. Executing a manipulation can lead to code injection. The attack may be performed from 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. | 2026-05-03 | 6.3 | CVE-2026-7700 |
| LifeSize--ClearSea | LifeSize ClearSea 3.1.4 contains directory traversal vulnerabilities that allow authenticated attackers to download and upload arbitrary files by manipulating path parameters in the smartgui interface. Attackers can exploit the upload endpoint with directory traversal sequences to write files to arbitrary locations on the system, enabling remote code execution. | 2026-04-29 | 6.5 | CVE-2018-25312 |
| mem0ai--mem0 | A vulnerability was found in mem0ai mem0 up to 1.0.11. This affects the function pickle.load/pickle.dump of the file mem0/vector_stores/faiss.py. Performing a manipulation results in deserialization. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The patch is named 62dca096f9236010ca15fea9ba369ba740b86b7a. Applying a patch is the recommended action to fix this issue. | 2026-05-01 | 6.3 | CVE-2026-7597 |
| Merge--Merge PACS | Merge PACS 7.0 contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized actions by crafting malicious HTML forms targeting the merge-viewer endpoint. Attackers can submit POST requests to /servlet/actions/merge-viewer/summary with login credentials to hijack user sessions and gain unauthorized access to the PACS system. | 2026-04-29 | 5.3 | CVE-2018-25298 |
| Milesight--MS-Cxx63-PD | A command injection vulnerability exists in the web server of specific firmware versions of Milesight cameras. | 2026-04-27 | 6.8 | CVE-2026-32649 |
| MIT--Kerberos 5 | In MIT Kerberos 5 (aka krb5) before 1.22.3, there is a NULL pointer dereference if an application calls gss_accept_sec_context() on a system with a NegoEx mechanism registered in /etc/gss/mech. An unauthenticated remote attacker can trigger this, causing the process to terminate in parse_nego_message. | 2026-04-28 | 5.9 | CVE-2026-40355 |
| MIT--Kerberos 5 | In MIT Kerberos 5 (aka krb5) before 1.22.3, there is an integer underflow and resultant out-of-bounds read if an application calls gss_accept_sec_context() on a system with a NegoEx mechanism registered in /etc/gss/mech. An unauthenticated | 2026-04-28 | 5.9 | CVE-2026-40356 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | remote attacker can trigger this, possibly causing the process to terminate in parse_message. | | | |
| n/a--<br>V2Board v1.7.4 | Cross-Site Scripting (XSS) in V2Board thru 1.7.4. The custom_html field in theme configuration is rendered using Blade unescaped output in public/theme/v2board/dashboard.blade.php. An admin can inject arbitrary JavaScript via the saveThemeConfig API. All site visitors execute the payload, enabling cookie theft, session hijacking, or phishing. | 2026-05-01 | 6.9 | CVE-2026-37503 |
| n/a--<br>V2Board v1.7.4 | Sensitive server_token exposed via GET parameter in V2Board thru 1.7.4. In app/Http/Controllers/Server/UniProxyController.php, the server authentication token is accepted via GET parameter transmission. The token appears in URLs such as /api/v1/server/UniProxy/user?token=SECRET, causing it to be recorded in web server access logs, browser history, HTTP Referer headers, and proxy/CDN logs. An attacker who gains access to any log source can extract the token and impersonate a proxy server node, potentially intercepting all user traffic. | 2026-05-01 | 5.3 | CVE-2026-37504 |
| n/a--<br>V2Board v1.7.4 | SQL Injection via ORDER BY clause in V2Board thru 1.7.4. In app/Http/Controllers/Admin/UserController.php, the sort parameter from user input is passed directly to User::orderBy($sort, $sortType) without validation. An authenticated admin can sort users by any database column including password, remember_token, and other sensitive fields, enabling information disclosure through ordering analysis. | 2026-05-01 | 4.9 | CVE-2026-37505 |
| n/a--crmeb_java | A vulnerability was detected in crmeb_java up to 1.3.4. This vulnerability affects unknown code of the file crmeb/crmeb-service/src/main/java/com/zbkj/service/service/impl/UploadServiceImpl.java of the component Admin Upload. Performing a manipulation of the argument model results in unrestricted upload. Remote exploitation of the attack is possible. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 4.7 | CVE-2026-7673 |
| n/a--JeecgBoot | A vulnerability was found in JeecgBoot up to 3.9.1. Affected by this vulnerability is an unknown functionality of the file /sys/fillRule/edit of the component FillRuleUtil Component. The manipulation of the argument ruleClass results in improper authorization. The attack may be performed from remote. The exploit has been made public and could be used. You should upgrade the affected component. The vendor confirmed the issue and will provide a fix in the upcoming release. | 2026-05-02 | 6.3 | CVE-2026-7602 |
| n/a--JeecgBoot | A vulnerability was determined in JeecgBoot up to 3.9.1. Affected by this issue is the function checkPathTraversalBatch of the file FileDownloadUtils.jav of the component LoadFile Endpoint. This manipulation of the argument files causes server-side request forgery. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The affected component should be upgraded. The vendor confirmed the issue and will provide a fix in the upcoming release. | 2026-05-02 | 6.3 | CVE-2026-7603 |
| n/a--JeecgBoot | A vulnerability was identified in JeecgBoot up to 3.9.1. This affects the function OpenApiController.add/OpenApiController.call of the file OpenApiController.java of the component OpenApi Service. Such manipulation of the argument originUrl database leads to server-side request forgery. It is possible to launch the attack remotely. The exploit is publicly available and might be used. It is suggested to upgrade the affected component. The vendor confirmed the issue and will provide a fix in the upcoming release. | 2026-05-02 | 6.3 | CVE-2026-7604 |
| n/a--JeecgBoot | A security flaw has been discovered in JeecgBoot up to 3.9.1. This vulnerability affects the function CommonController.uploadImgByHttp/HttpFileToMultipartFileUtil.httpFileToMultipartFile/HttpFileToMultipartFileUtil.downloadImageData of the file CommonController.java of the component uploadImgByHttpEndpoint. Performing a manipulation results in server-side request forgery. The attack can be initiated | 2026-05-02 | 6.3 | CVE-2026-7605 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | remotely. The exploit has been released to the public and may be used for attacks. Upgrading the affected component is recommended. The vendor confirmed the issue and will provide a fix in the upcoming release. | | | |
| n/a--MindsDB | A security vulnerability has been detected in MindsDB up to 26.01. Affected is the function pickle.loads of the component Pickle Handler. The manipulation leads to deserialization. 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. | 2026-05-03 | 6.3 | CVE-2026-7712 |
| n/a--Open5GS | A vulnerability has been found in Open5GS up to 2.7.6. Affected is an unknown function of the file src/amf/gmm-handler.c of the component AMF. The manipulation of the argument reg_type leads to denial of service. The attack is possible to be carried out remotely. Upgrading to version 2.7.7 is able to address this issue. The identifier of the patch is ebc66942b6f8f1fab2d640e71cf4e9f1a423b426. It is advisable to upgrade the affected component. | 2026-05-02 | 4.3 | CVE-2026-7601 |
| n/a--Open5GS | A vulnerability has been found in Open5GS up to 2.7.7. This issue affects the function gmm_handle_service_request of the file /src/amf/gmm-handler.c of the component AMF. The manipulation leads to denial of service. 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. | 2026-05-03 | 4.3 | CVE-2026-7706 |
| n/a--Open5GS | A vulnerability was found in Open5GS up to 2.7.7. Impacted is the function udr_nudr_dr_handle_subscription_context of the file /src/udr/nudr-handler.c of the component UDR. The manipulation of the argument pei results in denial of service. The attack can be launched remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet. | 2026-05-03 | 4.3 | CVE-2026-7707 |
| n/a--Open5GS | A vulnerability was determined in Open5GS up to 2.7.7. The affected element is the function ogs_dbi_subscription_data in the library /lib/dbi/subscription.c of the component UDR. This manipulation of the argument supi_id causes denial of service. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet. | 2026-05-03 | 4.3 | CVE-2026-7708 |
| nextlevelbuilder--ui-ux-pro-max-skill | A flaw has been found in nextlevelbuilder ui-ux-pro-max-skill up to 2.5.0. Affected by this vulnerability is the function _format_plugins of the file .claude/skills/ui-styling/scripts/tailwind_config_gen.py of the component Tailwind Config Generator. This manipulation causes code injection. The attack is possible to be carried out remotely. The exploit has been published and may be used. The project was informed of the problem early through a pull request but has not reacted yet. | 2026-05-01 | 6.3 | CVE-2026-7595 |
| nextlevelbuilder--ui-ux-pro-max-skill | A vulnerability has been found in nextlevelbuilder ui-ux-pro-max-skill up to 2.5.0. Affected by this issue is the function data.get of the file .claude/skills/design-system/scripts/generate-slide.py of the component Slide Generator. Such manipulation leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through a pull request but has not reacted yet. | 2026-05-01 | 4.3 | CVE-2026-7596 |
| Oracle Corporation--Oracle Linux | An unprivileged attacker can craft a user-space process with a malicious ELF binary containing an out-of-range sh_link field. When root-level dtrace attaches to -- or instruments -- that process (via dtrace -p , pid probes, or USDT), the ELF parser reads heap memory beyond the allocated section cache array without any bounds check. This results in an uninitialized/out-of-bounds heap read that can cause a NULL pointer dereference crash of the dtrace process (DoS), or -- depending on heap layout -- a read-then-use of a garbage pointer controlled by adjacent | 2026-05-01 | 4.4 | CVE-2026-35233 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | allocations, providing a foothold toward further exploitation in a privileged context. | | | |
| poppler-utils--PDFunite | PDFunite 0.41.0 contains a buffer overflow vulnerability that allows local attackers to crash the application by processing malformed PDF files during merge operations. Attackers can trigger a segmentation fault in the XRef::getEntry function within libpoppler by providing a specially crafted PDF file to the pdfunite utility. | 2026-04-29 | 6.2 | CVE-2018-25306 |
| pskill9--website-downloader | A vulnerability was detected in pskill9 website-downloader up to 0.1.0. This affects the function download_website of the file src/index.ts of the component MCP Interface. Performing a manipulation of the argument outputPath results in os command injection. The attack may be initiated remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet. | 2026-05-02 | 6.3 | CVE-2026-7642 |
| r-huijts--mcp-server-rijksmuseum | A security flaw has been discovered in r-huijts mcp-server-rijksmuseum up to 1.0.4. Affected is the function open_image_in_browser of the file src/index.ts of the component MCP Interface. Performing a manipulation of the argument imageUrl results in os 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 project was informed of the problem early through an issue report but has not responded yet. | 2026-05-02 | 6.3 | CVE-2026-7653 |
| redhat[.]com--gnutls | A flaw was found in gnutls. This vulnerability occurs because gnutls performs case-sensitive comparisons of `nameConstraints` labels, specifically for `dNSName` (DNS) or `rfc822Name` (email) constraints within `excludedSubtrees` or `permittedSubtrees`. A remote attacker can exploit this by crafting a leaf certificate with casing differences in the Subject Alternative Name (SAN), leading to a policy bypass where a certificate that should be rejected is instead accepted. This could result in unauthorized access or information disclosure. | 2026-04-30 | 6.5 | CVE-2026-3833 |
| ruvnet--sublinear-time-solver | A vulnerability was found in ruvnet sublinear-time-solver 1.5.0. Affected by this vulnerability is the function export_state of the file src/consciousness-explorer/mcp/server.js of the component MCP Interface. The manipulation results in path traversal. 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. | 2026-05-02 | 6.5 | CVE-2026-7645 |
| sebet--Go Fetch Jobs (for WP Job Manager) | Multiple plugins and/or themes for WordPress are vulnerable to Reflected Cross-Site Scripting via the url parameter in various versions 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. | 2026-05-01 | 6.1 | CVE-2024-13362 |
| sgl-project--SGLang | A vulnerability was detected in sgl-project SGLang up to 0.5.9. Impacted is the function get_tokenizer of the file python/sglang/srt/utils/hf_transformers_utils.py of the component HuggingFace Transformer Handler. The manipulation of the argument trust_remote_code with the input False as part of Boolean results in code injection. The attack can be executed remotely. A high complexity level is associated with this attack. The exploitability is considered difficult. In get_tokenizer(), when the caller passes trust_remote_code=False and HuggingFace transformers v5 returns a TokenizersBackend instance (the generic fallback for tokenizer classes not in the registry), SGLang silently re-invokes AutoTokenizer.from_pretrained with trust_remote_code=True, overriding the caller's explicit security setting. A model repository containing a malicious tokenizer.py referenced via auto_map in tokenizer_config.json will execute arbitrary Python in the SGLang process during this second call. No log line or warning is emitted. The override affects all current SGLang versions because transformers==5.3.0 is pinned in pyproject.toml. Both tokenizer_mode="auto" and tokenizer_mode="slow" are affected. The exploit is now public and may be used. | 2026-05-02 | 5.6 | CVE-2026-7669 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | The vendor was contacted early about this disclosure but did not respond in any way. | | | |
| SmarterTools Inc.--SmarterMail | SmarterTools SmarterMail builds prior to 9610 contain a cryptographic weakness in the file and email sharing endpoints that use DES-CBC encryption with keys and initialization vectors derived from System.Random seeded with insufficient entropy, reducing the seed space to approximately 19,000 possible values. An unauthenticated attacker can use the attachment download endpoint as an oracle to determine the seed in use and derive encryption keys and initialization vectors to forge sharing tokens for arbitrary emails, attachments, or file storage contents without prior access to the targeted content. | 2026-04-27 | 5.9 | CVE-2026-40514 |
| Sysgauge--SysGauge | SysGauge 4.5.18 contains a buffer overflow vulnerability in the proxy configuration handler that allows local attackers to cause a denial of service by supplying an oversized string. Attackers can inject a large payload through the Proxy Server Host Name field in the Options menu to crash the application. | 2026-04-29 | 6.2 | CVE-2018-25313 |
| Telegram--Desktop | A security vulnerability has been detected in Telegram Desktop up to 6.7.5. This vulnerability affects the function RequestButton of the file Telegram/SourceFiles/boxes/url_auth_box.cpp of the component Bot API. The manipulation of the argument login_url leads to null pointer dereference. It is possible to initiate the attack 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. | 2026-05-03 | 4.3 | CVE-2026-7701 |
| toeverything--AFFiNE | A vulnerability was detected in toeverything AFFiNE up to 0.26.3. This issue affects the function allowDocPreview of the file /workspace/:workspaceId/:docId of the component Public Markdown Preview Endpoint. The manipulation results in authorization bypass. It is possible to launch the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 5.3 | CVE-2026-7702 |
| Totolink--N300RH | A vulnerability was identified in Totolink N300RH 6.1c.1353_B20190305. This impacts the function setUploadSetting of the file /cgi-bin/cstecgi.cgi. Such manipulation of the argument FileName leads to file inclusion. The attack may be performed from remote. The exploit is publicly available and might be used. | 2026-05-02 | 6.5 | CVE-2026-7633 |
| TRENDnet--TEW-821DAP | A flaw has been found in TRENDnet TEW-821DAP up to 1.12B01. The impacted element is the function tools_diagnostic of the file /tmp/diagnostic of the component Firmware Udpate. This manipulation causes os command injection. Remote exploitation of the attack is possible. The exploit has been published and may be used. The vendor explains: "That firmware version will only work on our hardware version v1.xR. We have already EOL that product 8 years ago and are no longer selling". This vulnerability only affects products that are no longer supported by the maintainer. | 2026-05-02 | 6.3 | CVE-2026-7609 |
| TRENDnet--TEW-821DAP | A vulnerability was detected in TRENDnet TEW-821DAP up to 1.12B01. The affected element is the function tools_diagnostic. The manipulation results in os command injection. The exploit is now public and may be used. The vendor explains: "That firmware version will only work on our hardware version v1.xR. We have already EOL that product 8 years ago and are no longer selling". This vulnerability only affects products that are no longer supported by the maintainer. | 2026-05-02 | 5.5 | CVE-2026-7608 |
| trustindex--Widgets for Social Photo Feed | The Widgets for Social Photo Feed plugin for WordPress is vulnerable to unauthorized access of data and modification of data due to a missing capability check on the '/trustindex_feed_hook_instagram/troubleshooting' and '/trustindex_feed_hook_instagram/submit-data' REST API endpoints in all versions up to, and including, 1.8. This makes it possible for unauthenticated attackers to access and update plugin settings. | 2026-05-02 | 6.5 | CVE-2025-14726 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| VideoFlow Ltd.--VideoFlow Digital Video Protection | VideoFlow Digital Video Protection DVP 2.10 contains an authenticated directory traversal vulnerability that allows authenticated attackers to disclose arbitrary files by injecting path traversal sequences in the ID parameter. Attackers can submit requests to downloadsys.pl, download_xml.pl, download.pl, downloadmib.pl, or downloadFile.pl with directory traversal payloads to read sensitive system files like /etc/passwd. | 2026-04-29 | 6.5 | CVE-2018-25311 |
| VideoFlow Ltd.--VideoFlow Digital Video Protection | VideoFlow Digital Video Protection DVP 2.10 contains an authenticated remote code execution vulnerability that allows authenticated attackers to execute arbitrary system commands by exploiting a cross-site request forgery flaw in the web management interface. Attackers with valid credentials can leverage the CSRF vulnerability to inject and execute system commands through the Tools > System > Shell interface, gaining root-level access to the device. | 2026-04-29 | 4.3 | CVE-2018-25310 |
| Wavlink--WL-WN570HA1 | A weakness has been identified in Wavlink WL-WN570HA1 R70HA1 V1410_221110. This issue affects the function set_sys_adm of the file /cgi-bin/adm.cgi. This manipulation of the argument Username causes command injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. Once again the vendors acted very professional and confirms, "that the WN570HA1 firmware version R70HA1 V1410_221110 has been removed from our website." This vulnerability only affects products that are no longer supported by the maintainer. | 2026-05-03 | 6.3 | CVE-2026-7690 |
| Wavlink--WL-WN570HA1 | A security vulnerability has been detected in Wavlink WL-WN570HA1 R70HA1 V1410_221110. Impacted is the function set_sys_cmd of the file /cgi-bin/adm.cgi. Such manipulation of the argument command leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. Once again the vendors acted very professional and confirms, "that the WN570HA1 firmware version R70HA1 V1410_221110 has been removed from our website." This vulnerability only affects products that are no longer supported by the maintainer. | 2026-05-03 | 6.3 | CVE-2026-7691 |
| Wavlink--WL-WN570HA1 | A vulnerability was detected in Wavlink WL-WN570HA1 R70HA1 V1410_221110. The affected element is the function ping_ddns of the file /cgi-bin/adm.cgi. Performing a manipulation of the argument DDNS results in command injection. The attack can be initiated remotely. The exploit is now public and may be used. Once again the vendors acted very professional and confirms, "that the WN570HA1 firmware version R70HA1 V1410_221110 has been removed from our website." This vulnerability only affects products that are no longer supported by the maintainer. | 2026-05-03 | 6.3 | CVE-2026-7692 |
| wazuh--wazuh | Wazuh is a free and open source platform used for threat prevention, detection, and response. From version 4.0.0 to before version 4.14.4, Wazuh's server API brute-force protection for POST /security/user/authenticate can be bypassed by sending concurrent authentication requests. Although the configured threshold (max_login_attempts, default 50) is enforced correctly for sequential requests, a parallel burst allows significantly more failed login attempts to be processed before the IP block is applied. This enables an attacker to perform more password guesses than the configured policy intends (e.g., 100 attempts processed where 50 should be allowed). This issue has been patched in version 4.14.4. | 2026-04-29 | 6.5 | CVE-2026-26206 |
| wazuh--wazuh | Wazuh is a free and open source platform used for threat prevention, detection, and response. From version 1.0.0 to before version 4.14.4, a heap-based out-of-bounds WRITE occurs in GetAlertData, resulting in writing a NULL byte exactly 1 byte before the start of the buffer allocated by strdup. Due to unsigned integer underflow and pointer arithmetic wrapping, the write lands at offset -1 from the buffer, corrupting heap metadata. A malicious actor can potentially leverage this issue through a compromised agent to cause denial of service or heap corruption by injecting a specially crafted alert into the alerts log file monitored by wazuh-logcollector. This issue has been patched in version 4.14.4. | 2026-04-29 | 4.4 | CVE-2026-26204 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| wproyal--Royal Addons for Elementor Addons and Templates Kit for Elementor | The Royal Addons for Elementor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `wpr_update_form_action_meta` AJAX action in all versions up to, and including, 1.7.1056. The handler is registered on both `wp_ajax` and `wp_ajax_nopriv` hooks, making it accessible to unauthenticated users. Although a nonce is verified, the nonce (`wpr-addons-js`) is publicly exposed in frontend JavaScript via `WprConfig.nonce` on any page that loads Royal Addons widgets, rendering the protection ineffective. The endpoint also lacks any capability or ownership checks and directly calls `update_post_meta()` with user-controlled input on a whitelisted set of form action meta keys. This makes it possible for unauthenticated attackers to modify form action configuration metadata (email, submissions, Mailchimp, and webhook settings) on any post, potentially leading to webhook/email action tampering and data exfiltration via modified webhook URLs. | 2026-05-02 | 5.3 | CVE-2026-4024 |
| WSO2--WSO2 Identity Server | The authentication endpoint accepts user-supplied input without enforcing expected validation constraints, leading to a lack of proper output encoding. This allows for the injection of malicious JavaScript payloads, enabling reflected cross-site scripting. An attacker can leverage this vulnerability to redirect the user's browser to a malicious website, modify the user interface of the web page, retrieve information from the browser, or cause other harmful actions. However, due to the protection of session-related cookies with the httpOnly flag, session hijacking is not possible. | 2026-04-29 | 6.1 | CVE-2025-10503 |
| xenial--RSVG | librsvg2-bin 2.40.13 contains a buffer overflow vulnerability that allows local attackers to cause a denial of service by processing malformed SVG files. Attackers can supply crafted SVG input to the rsvg conversion tool to trigger a segmentation fault in the cairo image compositor. | 2026-04-29 | 6.2 | CVE-2018-25305 |
| xlplugins--NextMove Lite Thank You Page for WooCommerce | The NextMove Lite - Thank You Page for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'xlwcty_current_date' shortcode in all versions up to, and including, 2.23.0 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. | 2026-05-02 | 6.4 | CVE-2026-0703 |
| youlaitech--youlai-boot | A security vulnerability has been detected in youlaitech youlai-boot up to 2.21.1. This affects the function getUserList of the file src/main/java/com/youlai/boot/system/controller/UserController.java of the component Users Endpoint. Such manipulation of the argument order leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 6.3 | CVE-2026-7672 |
| YunaiV--yudao-cloud | A vulnerability was identified in YunaiV yudao-cloud up to 2026.01. This affects the function getDataBySQL of the file yudao-module-report-biz/src/main/java/io/github/ruoyi/report/service/impl/GoViewDataServiceImpl.java. Such manipulation leads to sql 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. | 2026-05-03 | 6.3 | CVE-2026-7678 |
| Zyxel--DX3300-T0 firmware | A post-authentication command injection vulnerability in the EasyMesh-related APIs of Zyxel DX3300-T0 firmware versions through 5.50(ABVY.7.1)C0 could allow an authenticated, adjacent attacker with administrator privileges to execute OS commands on an affected device. | 2026-04-28 | 6.8 | CVE-2026-0711 |

# Low Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Dell--PowerProtect Agent | Dell PowerProtect Agent Service, version(s) prior to 20.1, contain(s) an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure. | 2026-04-08 | 3.3 | CVE-2026-28264 |
| electron--electron | Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. From 33.0.0-alpha.1 to before 39.8.5, 40.8.5, 41.1.0, and 42.0.0-alpha.5, apps that use offscreen rendering with GPU shared textures may be vulnerable to a use-after-free. Under certain conditions, the release() callback provided on a paint event texture can outlive its backing native state, and invoking it after that point dereferences freed memory in the main process, which may lead to a crash or memory corruption. Apps are only affected if they use offscreen rendering with webPreferences.offscreen: { useSharedTexture: true }. Apps that do not enable shared-texture offscreen rendering are not affected. To mitigate this issue, ensure texture.release() is called promptly after the texture has been consumed, before the texture object becomes unreachable. This vulnerability is fixed in 39.8.5, 40.8.5, 41.1.0, and 42.0.0-alpha.5. | 2026-04-06 | 2.3 | CVE-2026-34764 |
| electron--electron | Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.5, 40.8.5, 41.1.0, and 42.0.0-alpha.5, apps that call clipboard.readImage() may be vulnerable to a denial of service. If the system clipboard contains image data that fails to decode, the resulting null bitmap is passed unchecked to image construction, triggering a controlled abort and crashing the process. Apps are only affected if they call clipboard.readImage(). Apps that do not read images from the clipboard are not affected. This issue does not allow memory corruption or code execution. This vulnerability is fixed in 39.8.5, 40.8.5, 41.1.0, and 42.0.0-alpha.5. | 2026-04-07 | 2.8 | CVE-2026-34781 |
| harttle--liquidjs | LiquidJS is a Shopify / GitHub Pages compatible template engine in pure JavaScript. Prior to 10.25.3, the replace filter in LiquidJS incorrectly accounts for memory usage when the memoryLimit option is enabled. It charges str.length + pattern.length + replacement.length bytes to the memory limiter, but the actual output from str.split(pattern).join(replacement) can be quadratically larger when the pattern occurs many times in the input string. This allows an attacker who controls template content to bypass the memoryLimit DoS protection with approximately 2,500x amplification, potentially causing out-of-memory conditions. This vulnerability is fixed in 10.25.3. | 2026-04-08 | 3.7 | CVE-2026-34166 |
| Mattermost--Mattermost | Mattermost Plugins versions <=2.3.1 fail to limit the request body size on the {{/lifecycle}} webhook endpoint which allows an authenticated attacker to cause memory exhaustion and denial of service via sending an oversized JSON payload. Mattermost Advisory ID: MMSA-2026-00610 | 2026-04-09 | 3.7 | CVE-2026-21388 |
| OpenStack--Keystone | An issue was discovered in OpenStack Keystone 14 through 26 before 26.1.1, 27.0.0, 28.0.0, and 29.0.0. Restricted application credentials can create EC2 credentials. By using a restricted application credential to call the EC2 credential creation API, an authenticated user with only a reader role may obtain an EC2/S3 credential that carries the full set of the parent user's S3 permissions, effectively bypassing the role restrictions imposed on the application credential. Only deployments that use restricted application credentials in combination with the EC2/S3 compatibility API (swift3 / s3api) are affected. | 2026-04-10 | 3.5 | CVE-2026-33551 |
| pi-hole--web | Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. From 6.0 to before 6.5, client hostnames and IP addresses from the FTL database are rendered into the DOM without escaping in network.js (Network page) and charts.js/index.js (Dashboard chart tooltips). While upstream validation in dnsmasq and FTL blocks HTML characters via normal DHCP/DNS paths, the web UI performs no output escaping - an | 2026-04-06 | 3.4 | CVE-2026-33404 |

# Low Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | inconsistency with other fields in the same file that are properly escaped. This vulnerability is fixed in 6.5. | | | |
| pi-hole--web | Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. From 6.0 to before 6.5, the formatInfo() function in queries.js renders data.upstream, data.client.ip, and data.ede.text into HTML without escaping when a user expands a query row in the Query Log, enabling stored HTML injection. JavaScript execution is blocked by the server's CSP (script-src 'self'). The same fields are properly escaped in the table view (rowCallback), confirming the omission was an oversight. This vulnerability is fixed in 6.5. | 2026-04-06 | 3.1 | CVE-2026-33405 |
| 1Panel-dev--MaxKB | A vulnerability has been found in 1Panel-dev MaxKB up to 2.4.2. Impacted is an unknown function of the file ui/src/chat.ts of the component MdPreview. Such manipulation leads to cross site scripting. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2.5.0 is recommended to address this issue. The name of the patch is 7230daa5ec3e6574b6ede83dd48a4fbc0e70b8d8. It is advisable to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product. | 2026-04-13 | 3.5 | CVE-2025-15632 |
| Fortinet--FortiNAC-F | An URL Redirection to Untrusted Site ('Open Redirect') vulnerability [CWE-601] vulnerability in Fortinet FortiNAC-F 7.6.0 through 7.6.5, FortiNAC-F 7.4 all versions, FortiNAC-F 7.2 all versions may allow a remote privileged attacker with system administrator role to redirect users to an arbitrary website via crafted CSV file. | 2026-04-14 | 2.2 | CVE-2026-21741 |
| Grafana--Grafana Correlations | --- title: Cross-Tenant Legacy Correlation Disclosure and Deletion draft: false hero: image: /static/img/heros/hero-legal2.svg content: "# Cross-Tenant Legacy Correlation Disclosure and Deletion" date: 2026-01-29 product: Grafana severity: Low cve: CVE-2026-21727 cvss_score: "3.3" cvss_vector: "CVSS:3.3/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N" fixed_versions: - ">=11.6.11 >=12.0.9 >=12.1.6 >=12.2.4" --- A cross-tenant isolation vulnerability was found in Grafana's Correlations feature affecting legacy correlation records. Due to a backward compatibility condition allowing org_id = 0 records to be returned across organizations, a user with datasource management privileges could read and permanently delete legacy correlation data belonging to another organization. This issue affects correlations created prior to Grafana 10.2 and is fixed in >=11.6.11, >=12.0.9, >=12.1.6, and >=12.2.4. Thanks to Gyu-hyeok Lee (g2h) for reporting this vulnerability. | 2026-04-15 | 3.3 | CVE-2026-21727 |
| HCL--AION | HCL AION is affected by a vulnerability where certain system behaviours may allow exploration of internal filesystem structures. Exposure of such information may provide insights into the underlying environment, which could potentially aid in further targeted actions or limited information disclosure. | 2026-04-15 | 2.9 | CVE-2025-52641 |
| Siemens--Siemens Software Center | A vulnerability has been identified in Siemens Software Center (All versions < V3.5.8.2), Simcenter 3D (All versions < V2506.6000), Simcenter Femap (All versions < V2506.0002), Simcenter STAR-CCM+ (All versions < V2602), Solid Edge SE2025 (All versions < V225.0 Update 13), Solid Edge SE2026 (All versions < V226.0 Update 04), Tecnomatix Plant Simulation (All versions < V2504.0008). Affected applications do not properly validate client certificates to connect to Analytics Service endpoint. This could allow an unauthenticated remote attacker to perform man in the middle attacks. | 2026-04-14 | 3.7 | CVE-2025-40745 |
| WSO2--WSO2 API Manager | The component accepts XML input through the publisher without disabling external entity resolution. This allows malicious actors to submit a crafted XML payload that exploits the unescaped external entity references. By leveraging this vulnerability, a malicious actor can read confidential files from the product's file system or access limited HTTP resources reachable via HTTP GET requests to the vulnerable product. | 2026-04-16 | 3.5 | CVE-2024-8010 |

# Low Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| HCLSoftware--BigFix Service Management (SM) | HCL BigFix Service Management is susceptible to HTTP Request Smuggling. HTTP request smuggling vulnerabilities arise when websites route HTTP requests through web servers with inconsistent HTTP parsing. HTTP Smuggling exploits inconsistencies in request parsing between front-end and back-end servers, allowing attackers to bypass security controls and perform attacks like cache poisoning or request hijacking. | 2026-04-21 | 3.7 | CVE-2025-31958 |
| CodeWise--Tornet Scooter Mobile App | A vulnerability has been found in CodeWise Tornet Scooter Mobile App 4.75 on iOS/Android. The impacted element is an unknown function of the file /TwoFactor. Such manipulation leads to improper restriction of excessive authentication attempts. The attack may be performed from remote. Attacks of this nature are highly complex. The exploitability is regarded as difficult. 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. | 2026-05-02 | 3.7 | CVE-2026-7671 |
| Dolibarr--ERP CRM | A security flaw has been discovered in Dolibarr ERP CRM up to 23.0.2. This vulnerability affects the function dol_verifyHash in the library htdocs/core/lib/security.lib.php of the component Online Signature Module. The manipulation results in improper verification of cryptographic signature. The attack may be performed from remote. Attacks of this nature are highly complex. It is stated that the exploitability is difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 3.7 | CVE-2026-7689 |
| kerwincui--FastBee | A vulnerability was determined in kerwincui FastBee up to 1.2.1. The impacted element is the function Add of the file springboot/fastbee-admin/src/main/java/com/fastbee/web/controller/system/SysNoticeController.java of the component System Notice Handler. This manipulation of the argument noticeContent causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way. | 2026-05-03 | 3.5 | CVE-2026-7677 |
| Oracle Corporation--Oracle Linux | An unprivileged attacker can reliably trigger a crash of the dtrace process with a malicious ELF binary due to an integer Divide-by-Zero in Pbuild_file_symtab() | 2026-05-01 | 3.3 | CVE-2026-21996 |
| redhat[.]com--gnutls | A flaw was found in gnutls. A remote attacker could exploit this vulnerability by presenting a specially crafted Online Certificate Status Protocol (OCSP) response during a TLS handshake. Due to a logic error in how gnutls processes multi-record OCSP responses, a client with OCSP verification enabled may incorrectly accept a revoked server certificate, potentially leading to a compromise of trust. | 2026-04-30 | 3.7 | CVE-2026-3832 |
| TRENDnet--TEW-821DAP | A weakness has been identified in TRENDnet TEW-821DAP 1.12B01. This issue affects the function find_hwid/new_gui_update_firmware of the component Firmware Update Handler. Executing a manipulation of the argument dest can lead to insufficient verification of data authenticity. The attack can be launched remotely. Attacks of this nature are highly complex. The exploitability is assessed as difficult. The vendor explains: "That firmware version will only work on our hardware version v1.xR. We have already EOL that product 8 years ago and are no longer selling". This vulnerability only affects products that are no longer supported by the maintainer. | 2026-05-02 | 3.7 | CVE-2026-7606 |
| TRENDnet--TEW-821DAP | A vulnerability has been found in TRENDnet TEW-821DAP 1.12B01. This affects an unknown function of the file /www/cgi/ssi of the component Firmware Update. Such manipulation leads to cleartext transmission of sensitive information. The attack can be executed remotely. This attack is characterized by high complexity. The exploitability is reported as difficult. The exploit has been disclosed to the public and may be used. The vendor explains: "That firmware version will only work on our hardware version v1.xR. We have already EOL that product 8 years ago and are no longer selling". This vulnerability only affects products that are no longer supported by the maintainer. | 2026-05-02 | 3.7 | CVE-2026-7610 |

# Low Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| TRENDnet--TEW-821DAP | A vulnerability was found in TRENDnet TEW-821DAP up to 1.12B01. This impacts the function platform_do_upgrade_cameo_dev of the file cameo_dev.sh of the component Firmware Update Handler. Performing a manipulation results in insufficient verification of data authenticity. The attack is possible to be carried out remotely. The complexity of an attack is rather high. The exploitability is said to be difficult. The vendor explains: "That firmware version will only work on our hardware version v1.xR. We have already EOL that product 8 years ago and are no longer selling". This vulnerability only affects products that are no longer supported by the maintainer. | 2026-05-02 | 3.7 | CVE-2026-7611 |