SingCERT
Singapore Cyber Emergency Response Team

# Security Bulletin 15 July 2026

Generated on 15 July 2026

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

| | |
|---|---|
| Critical | vulnerabilities with a base score of 9.0 to 10.0 |
| High | vulnerabilities with a base score of 7.0 to 8.9 |
| Medium | vulnerabilities with a base score of 4.0 to 6.9 |
| Low | vulnerabilities with a base score of 0.1 to 3.9 |
| None | vulnerabilities with a base score of 0.0 |

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

## CRITICAL VULNERABILITIES

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2026-59726 | Ruflo is an agent meta-harness for Claude Code and Codex. Prior to 3.16.3, ruflo's default docker-compose deployment exposed the MCP bridge POST /mcp and POST /mcp/:group endpoints without authentication, allowing an unauthenticated network attacker to invoke tools/call to terminal_execute, obtain a shell in the bridge container, read provider API keys, and poison AgentDB learning-store patterns. This issue is fixed in version 3.16.3. | 10.0 | More Details |
| CVE-2026-57811 | Improper Control of Generation of Code ('Code Injection') vulnerability in Realtyna Realtyna Organic IDX plugin real-estate-listing-realtyna-wpl allows Remote Code Inclusion.This issue affects Realtyna Organic IDX plugin: from n/a through <= 5.2.0. | 10.0 | More Details |
| CVE-2026-57719 | Unrestricted Upload of File with Dangerous Type vulnerability in CodeRevolution Aimogen Pro aimogen-pro allows Using Malicious Files.This issue affects Aimogen Pro: from n/a through <= 2.8.3. | 10.0 | More Details |
| CVE-2026-54769 | Langroid is a framework for building large-language-model-powered applications. Versions prior to 0.65.2 are vulnerable to a critical Sandbox Escape leading to Remote Code Execution (RCE) in its `TableChatAgent` and `VectorStore` capabilities. When these agents evaluate LLM-generated tool messages with `full_eval=True`, they attempt to sandbox the execution by explicitly setting `locals` to an empty dictionary `{}` inside Python's `eval()` function. However, this relies on an incomplete understanding of Python's execution model. Because `__builtins__` is not explicitly scrubbed from the `globals` dictionary mapping, Python implicitly injects all built-ins during execution, granting full access to functions like `__import__('os').system()`. Since `TableChatAgent.pandas_eval()` executes external LLM outputs natively, this bypass permits any attacker providing prompt payload to achieve unauthenticated RCE on the host system. Version 0.65.2 patches the issue. | 10.0 | More Details |
| CVE-2026-61447 | PraisonAI before 1.6.78 contains a remote code execution vulnerability in CodeAgent._execute_python() that executes LLM-generated Python code without AST validation, import restrictions, or sandbox enforcement. Attackers can influence LLM output through prompt injection to exfiltrate all environment secrets and execute arbitrary code on the host system. | 10.0 | More Details |
| CVE-2026-54782 | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, CoreWCF SAML 1.1 and SAML 2.0 token validation does not correctly resolve the issuer signing key or require signed tokens when IdentityConfiguration is used with federated bindings, allowing an unauthenticated remote attacker to impersonate any principal the trusted STS could issue. This issue is fixed in versions 1.8.1 and 1.9.1. | 10.0 | More Details |
| CVE-2026-62422 | In JetBrains YouTrack before 2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, 2024.2.148429 authentication bypass via direct database access leading to administrative access was possible | 10.0 | More Details |
| CVE-2026-56451 | A vulnerability has been identified in Opcenter X (All versions < V2604). Affected applications do not properly validate the algorithm specified in the JSON Web Token (JWT) header. This could allow an unauthenticated remote attacker to forge arbitrary JWT, bypass authentication mechanisms and impersonate any user including administrative accounts, potentially gaining full unauthorized access to the application. | 10.0 | More Details |
| CVE-2026-44747 | SAP NetWeaver Application Server ABAP allows an authenticated attacker to leverage logical errors in memory management to cause a memory corruption that could lead to unauthorized data access, modification, or system unavailability. This has high impact on confidentiality, integrity, and availability of the application. | 9.9 | More Details |
| CVE-2026-59827 | Metabase is an open-source business intelligence and embedded analytics tool. Prior to 1.58.15, 1.59.12, 1.60.6.3, and 1.61.1.4, Metabase instances with an H2 database connection, including the default sample database, deserialize arbitrary Java objects returned in H2 native query result columns of type OTHER without validation, allowing an authenticated user who can run native H2 queries to execute code on the Metabase server. This issue is fixed in versions 1.58.15, 1.59.12, 1.60.6.3, and 1.61.1.4. | 9.9 | More Details |
| CVE-2026-0284 | An XML injection vulnerability in the Large Scale VPN (LSVPN) functionality of Palo Alto Networks PAN-OS® software enables an unauthenticated attacker with network access to inject malicious XML content, potentially leading to information disclosure or corruption of internal LSVPN satellite data. Panorama, Cloud NGFW, and Prisma® Access are not impacted by this vulnerability. | 9.9 | More Details |

| | | | |
|---|---|---|---|
| CVE-2026-57710 | Unrestricted Upload of File with Dangerous Type vulnerability in quantumcloud WoowBot Pro Max woowbot-pro-max allows Using Malicious Files.This issue affects WoowBot Pro Max: from n/a through <= 14.1.7. | 9.9 | More Details |
| CVE-2026-57401 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Brainstorm Force SureDash suredash allows Path Traversal.This issue affects SureDash: from n/a through <= 1.8.0. | 9.9 | More Details |
| CVE-2026-56843 | Incorrect authorization in the XML-RPC API of WebPros Plesk before 18.0.78.4 allows a low-privileged authenticated customer to look up domains they do not own, because ownership is enforced only for certain lookup filters and schema validation is bypassed for legacy protocol versions. This results in cross-tenant disclosure of other tenants' FTP credentials stored in cleartext, which can be leveraged to execute code as another tenant's system user. | 9.9 | More Details |
| CVE-2026-14480 | OpenPLC Runtime v3 contains an authenticated arbitrary file write vulnerability in the legacy web UI program-upload workflow. The application stores an attacker-supplied filename (prog_file) directly into the Programs.File database field and later uses this value as the destination path for an uploaded file without validating or restricting the path. Because Python os.path.join() honors attacker-controlled absolute paths, an authenticated user can write arbitrary files anywhere writable by the OpenPLC webserver process. In the default build pipeline, all C++ source files within the OpenPLC runtime core directory are automatically compiled into the executable runtime binary. By writing a malicious .cpp file into this directory, an authenticated attacker can escalate the arbitrary file write into arbitrary native code execution when the operator triggers a normal program compilation and runtime start. | 9.9 | More Details |
| CVE-2026-55500 | 9Router is an AI router & token saver. Prior to 0.4.80, the /api/settings/database endpoint allows full database export (containing all credentials, API keys, OAuth tokens, and settings) and full database import (complete overwrite) without any authentication requirement beyond the ALWAYS_PROTECTED middleware check, which only validates JWT or CLI token. This issue is fixed in version 0.4.80. | 9.9 | More Details |
| CVE-2026-61445 | PraisonAI before 4.6.78 contains arbitrary file write and command execution vulnerabilities in the AICoder component due to missing path validation and command sanitization in LLM tool calls. Attackers can inject malicious prompts through the chat interface to write files to arbitrary filesystem locations and execute arbitrary shell commands with root privileges. | 9.9 | More Details |
| CVE-2026-60090 | PraisonAI before 4.6.78 fails to validate the caller-controlled dimension argument in the PGVector and Cassandra knowledge-store create_collection() backends. Although schema, keyspace, and collection-name identifiers are validated, the dimension value (declared as int but not enforced at runtime) is interpolated directly into the vector column of the generated CREATE TABLE DDL. A caller able to influence collection-creation dimensions can pass a string such as '3); DROP TABLE tenant_secrets; --' to inject SQL/CQL tokens into the statement executed by the database driver. | 9.8 | More Details |
| CVE-2026-57738 | Deserialization of Untrusted Data vulnerability in axiomthemes 777 triple-seven allows Object Injection.This issue affects 777: from n/a through <= 1.13.0. | 9.8 | More Details |
| CVE-2026-57827 | The Joomla extension RSFiles is vulnerable to an unauthenticated arbitrary file upload that allows uploading executable files and leads to full RCE. | 9.8 | More Details |
| CVE-2026-20744 | The charging station websocket endpoint accepts connections without proper authentication, which could lead to privilege escalation. | 9.8 | More Details |
| CVE-2026-56271 | Flowise before 3.1.0 (affected versions 3.0.13 and earlier) uses weak hardcoded default JWT secrets ('auth_token', 'refresh_token') and default audience and issuer values ('AUDIENCE', 'ISSUER') in the enterprise passport authentication middleware (packages/server/src/enterprise/middleware/passport/index.ts). When the corresponding environment variables (JWT_AUTH_TOKEN_SECRET, JWT_REFRESH_TOKEN_SECRET, JWT_AUDIENCE, JWT_ISSUER) are not set, the application silently falls back to these publicly known defaults, allowing an attacker to forge valid JWTs and impersonate any user, including administrators, resulting in authentication bypass. | 9.8 | More Details |
| CVE-2026-15511 | A vulnerability was determined in Comfast CF-WR631AX V3 up to 2.7.0.8. Affected by this vulnerability is the function system_wl_upload_pic_file of the file /usr/bin/webmgnt of the component FastCGI Backend. This manipulation of the argument filename causes os command injection. 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. | 9.8 | More Details |
| CVE-2026-4769 | Certain devices in the WAGO System I/O Field series activate an internal diagnostic capability during the initial startup sequence. This functionality is not formally documented and becomes accessible without authentication for a brief period in the early boot phase. During this window, an unauthenticated remote attacker can gain access to the internal system processes, resulting in full system compromise. | 9.8 | More Details |
| CVE-2026-11913 | vulnerability in Drupal Mother May I allows . This issue affects Mother May I versions: *.*. | 9.8 | More Details |
| CVE-2026-12535 | Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Formatter Field allows Object Injection. This issue affects Formatter Field versions: from 0.0.0 to 2.0.0. | 9.8 | More Details |
| CVE-2026-57724 | Deserialization of Untrusted Data vulnerability in Themeum Kirki kirki allows Object Injection.This issue affects Kirki: from n/a through <= 6.0.12. | 9.8 | More Details |
| CVE-2026-10768 | Missing Authorization vulnerability in Drupal LocalGov Workflows allows Forceful Browsing. This issue affects LocalGov Workflows versions: from 0.0.0 to 1.6.0. | 9.8 | More Details |
| CVE-2026-9726 | Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Drupal AlternativeCommerce (Basket) allows Object Injection. This issue affects Drupal AlternativeCommerce (Basket) versions: from 0.0.0 to 2.1.17. | 9.8 | More Details |
| CVE-2026-57807 | Authentication Bypass Using an Alternate Path or Channel vulnerability in miniOrange Security Software Pvt Ltd. OAuth Single Sign On - SSO (OAuth Client) allows Password Recovery Exploitation. This issue affects OAuth Single Sign On - SSO (OAuth Client): from n/a through 38.5.8. | 9.8 | More Details |
| CVE-2026-57770 | Deserialization of Untrusted Data vulnerability in ThemeGoods Grand Photography grandphotography allows Object Injection.This issue affects Grand Photography: from n/a through <= 5.7.8. | 9.8 | More Details |
| CVE-2026-57744 | Deserialization of Untrusted Data vulnerability in stmcan RT-Theme 18 \| Extensions rt18-extensions allows Object Injection.This issue affects RT-Theme 18 \| Extensions: from n/a through <= 2.5. | 9.8 | More Details |
| | DBI::SQL::Nano versions from 1.42 before 1.651 for Perl have inverted <= and >= SQL operators on text. DBI::SQL::Nano, DBI's built-in mini-SQL engine, evaluated WHERE predicates incorrectly in some cases. In the non-numeric string branch of the | | |

| | | | |
|---|---|---|---|
| CVE-2026-15043 | is_matched method, <= was evaluated using Perl's ge operator, and >= was evaluated using Perl's le operator. SQL::Nano is the fallback query engine for DBI's file-backed drivers (DBD::File, DBD::DBM, CSV-style drivers) whenever SQL::Statement is not installed, and is forced whenever DBI_SQL_NANO=1. Queries over such tables use these predicates directly. The impact depends on the context. Where an application relies on a WHERE clause to filter file-backed data for policy or authorization, an inverted <=/>= comparison silently returns the wrong rows. | 9.8 | More Details |
| CVE-2026-58644 | Deserialization of untrusted data in Microsoft Office SharePoint allows an unauthorized attacker to execute code over a network. | 9.8 | More Details |
| CVE-2026-54990 | Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network. | 9.8 | More Details |
| CVE-2026-50522 | Deserialization of untrusted data in Microsoft Office SharePoint allows an unauthorized attacker to execute code over a network. | 9.8 | More Details |
| CVE-2026-49172 | Heap-based buffer overflow in Windows FTP Service allows an unauthorized attacker to execute code over a network. | 9.8 | More Details |
| CVE-2026-42990 | Heap-based buffer overflow in SQL Server ODBC driver allows an unauthorized attacker to execute code over a network. | 9.8 | More Details |
| CVE-2026-15701 | A weakness has been identified in Totolink NR1800X 9.1.0u.6279_B20210910. Affected by this issue is the function Form_Logout of the file /formLogout.htm of the component lighttpd. This manipulation of the argument Host causes stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. | 9.8 | More Details |
| CVE-2026-58479 | Sustainable Irrigation Platform (SIP) through version 5.2.16 contains a command injection vulnerability in the optional cli_control plugin that allows unauthenticated or cross-site request forgery attackers to execute arbitrary operating-system commands by storing a malicious payload via the plugin's HTTP endpoint. Attackers can trigger execution by activating the associated irrigation station, exploiting the absence of passphrase protection or the default passphrase 'opendoor', to achieve arbitrary command execution on the underlying host. | 9.8 | More Details |
| CVE-2026-62392 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Apache Kylin. A backend API may bring job config parameters to OS command line. This issue affects Apache Kylin: from 4 through 5.0.3. Users are recommended to upgrade to version 5.0.4, which fixes the issue. | 9.8 | More Details |
| CVE-2026-62390 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Kylin. A backend API refreshing table catalog may cause the injection to the generated SQL. This issue affects Apache Kylin: from 4 through 5.0.3. Users are recommended to upgrade to version 5.0.4, which fixes the issue. | 9.8 | More Details |
| CVE-2026-59801 | 9Router through version 0.4.41 contains an unauthenticated access vulnerability that allows remote attackers to interact with provider management API endpoints by sending requests without any credentials due to missing authentication middleware in the Next.js API routes under src/app/api/providers/*. Attackers can enumerate, create, modify, or delete provider connections to expose partial credentials, OAuth tokens, and API keys, redirect AI traffic to attacker-controlled servers, or cause complete denial of service by deleting all provider connections. | 9.8 | More Details |
| CVE-2026-57156 | FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.28.0 on 32-bit builds, FreeRDP clients contain an integer overflow in update_read_delta_points in libfreerdp/core/orders.c when multiplying an attacker-controlled point count by sizeof(DELTA_POINT), allowing a malicious RDP peer to allocate an undersized heap buffer and then write beyond it during initialization. This issue is fixed in version 3.28.0. | 9.8 | More Details |
| CVE-2026-52533 | An issue in D-Link DIR-1253 v.1.0.1.250923.142435 allows an attacker to escalate privileges via the etc/shadow component file | 9.8 | More Details |
| CVE-2026-51821 | SQL Injection vulnerability in Shenzhou Shihan Video Conference System v.1.0 allows a remote attacker to execute arbitrary code via the /user/getUserLogin endpoint | 9.8 | More Details |
| CVE-2026-51540 | OpENer 2.3.0 (master branch up to commit 76b95cf) is vulnerable to a severe memory corruption issue caused by an integer underflow in the processing of connected explicit messages (SendUnitData). | 9.8 | More Details |
| CVE-2026-61500 | Rejetto HFS 3.0.0 through 3.2.0 derives its session-cookie signing key from the non-cryptographic Math.random() generator and discloses outputs of the same generator to unauthenticated clients during login. A remote attacker can collect a small number of login responses, reconstruct the generator's state, recover the signing key, and forge a valid administrator session cookie, leading to full administrative access and remote code execution via the server_code configuration feature. | 9.8 | More Details |
| CVE-2026-57433 | Storable versions before 3.41 for Perl have a signed integer overflow when deserializing a crafted SX_HOOK record. retrieve_hook_common reads a signed 32-bit item count from an SX_HOOK record and calls av_extend with that count plus one. A count of I32_MAX wraps the addition to a negative value. A crafted blob passed to thaw or retrieve triggers the overflow; av_extend receives the negative count and dies with a panic, terminating the deserialization. | 9.8 | More Details |
| CVE-2026-61498 | Vitec Flamingo 4.12.2 contains an unauthenticated OS command injection vulnerability in the admin/ajax/gen_graphs.php endpoint that allows remote unauthenticated attackers to execute arbitrary commands by supplying shell metacharacters in the start, end, key, or format HTTP GET parameters. Attackers can exploit the lack of input sanitization in the graph generation script, which passes user-supplied values directly to shell commands via passthru(), to execute arbitrary OS commands with root privileges due to the web server context having passwordless sudo access. | 9.8 | More Details |
| CVE-2026-60121 | Vitec Flamingo 4.12.2 contains an unauthenticated OS command injection vulnerability in the admin/ajax/ping.php endpoint that allows remote attackers to execute arbitrary commands by exploiting a double-evaluation flaw in shell argument handling. The endpoint applies escapeshellarg() to the user-supplied host POST parameter before passing it to a system wrapper, but the wrapper retrieves the decoded value from argv and incorporates it into a second shell_exec() call without escaping, allowing injected commands to execute with root privileges via passwordless sudo. | 9.8 | More Details |
| CVE-2026-59518 | Deserialization of Untrusted Data vulnerability in wpWax Directorist directorist allows Object Injection.This issue affects Directorist: from n/a through <= 8.8.2. | 9.8 | More Details |
| CVE-2026-57813 | Incorrect Privilege Assignment vulnerability in properfraction MailOptin mailoptin allows Privilege Escalation.This issue affects MailOptin: from n/a through <= 1.2.77.3. | 9.8 | More Details |
| | The miniOrange Social Login and Register (Discord, Google, Twitter, LinkedIn) plugin for WordPress is vulnerable to | | |

| | | | |
|---|---|---|---|
| CVE-2026-12761 | authentication bypass leading to account takeover in versions up to and including 7.7.0. This is due to the Profile Completion flow accepting an arbitrary email address via the 'email_field' POST parameter without verifying that the email belongs to the identity returned by the OAuth provider, combined with send_otp_token() returning the SHA-512(customer_key \|\| otp) transaction hash to the client where the OTP space is only 99,000 values (wp_rand(1000, 99999)) and the customer_key is a static option (empty on unregistered installs). This makes it possible for unauthenticated attackers to trigger an OTP email to an arbitrary admin's address, crack the OTP offline from the leaked hash in under a second, and submit the cracked OTP to mo_openid_social_login_validate_otp(), which logs the attacker in as the user whose email was supplied — granting full administrator access. | 9.8 | More Details |
| CVE-2026-50447 | Heap-based buffer overflow in Windows Message Queuing allows an unauthorized attacker to execute code over a network. | 9.8 | More Details |
| CVE-2026-5955 | Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Inrove Software and Internet Services BiEticaret allows SQL Injection. This issue affects BiEticaret: before v3.3.57. | 9.8 | More Details |
| CVE-2026-9695 | An Improper Authentication vulnerability affecting DELMIA Apriso from Release 2020 through Release 2026 could allow an attacker to gain privileged access to the server. | 9.8 | More Details |
| CVE-2026-14245 | The miniOrange OTP Login, Verification and SMS Notifications plugin for WordPress is vulnerable to Authentication Bypass leading to Administrator Account Takeover in all versions up to, and including, 5.5.1. This is due to the `um_reset_password_process_hook()` function performing no server-side verification that the OTP validation step was completed, and relying solely on a public `form_nonce` nonce that the plugin itself emits to unauthenticated visitors via the `moumprvar` JavaScript object on the Ultimate Member password reset page, while still accepting the attacker-controlled `username_b` parameter to target any WordPress user without role restriction or any binding to a previously validated OTP session. This makes it possible for unauthenticated attackers to obtain a freshly generated password-reset URL for an arbitrary Administrator account — returned in a 302 `Location` header — and use it to take full control of that account. Exploitation requires the Ultimate Member Password Reset Form integration to be active and the plugin to not be configured for phone-only reset. | 9.8 | More Details |
| CVE-2026-44024 | Fluentd collects events from various data sources and writes them to files, RDBMS, NoSQL, IaaS, SaaS, Hadoop and so on. Prior to 1.19.3, Fluentd allows dynamically constructing file paths using the ${tag} placeholder, and insufficient validation of ${tag} in file configurations such as the path parameter of the out_file plugin allows attackers sending untrusted tags containing path traversal characters to write or overwrite arbitrary files and potentially achieve remote code execution. This issue is fixed in version 1.19.3. | 9.8 | More Details |
| CVE-2026-15158 | The Blocksy Companion plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 2.1.46 via the save_attachments function. This is due to the Custom Fonts extension registering a wp_check_filetype_and_ext filter that approves any filename containing .woff2 or .ttf as a substring via strpos() rather than validating that those strings appear as the final extension via PATHINFO_EXTENSION — allowing double-extension filenames such as shell.woff2.php to pass MIME validation and be handled as permitted font files. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible. This vulnerability is only exploitable when the premium version of the plugin (blocksy-companion-pro) is installed with both the WooCommerce Extra (Advanced Reviews) and Custom Fonts extensions active; the free blocksy-companion plugin does not contain the vulnerable code paths. | 9.8 | More Details |
| CVE-2026-61459 | MCP Server Kubernetes before 3.9.0 contains an argument injection vulnerability in structured tools (kubectl_get, kubectl_describe, kubectl_delete) that allows attackers to bypass the assertNoDangerousFlags security check by supplying resourceType and name parameters with leading dashes. Attackers can inject the --server flag to redirect kubectl commands to an attacker-controlled API server, causing the operator's bearer token to be transmitted externally and enabling full cluster compromise. | 9.8 | More Details |
| CVE-2026-56291 | The Joomla extension Balbooa Forms is vulnerable to an unauthenticated arbitrary file upload that allows uploading executable files and leads to full RCE. | 9.8 | More Details |
| CVE-2026-12116 | A vulnerability in the Xerte Online Tools allows for RCE through the antivirus binary path in the tools server settings, which can be changed to a PHP interpreter, allowing an attacker to upload PHP data that will then be executed. | 9.8 | More Details |
| CVE-2026-58480 | Blocksy Companion Pro plugin for WordPress before 2.1.47 contains an unauthenticated arbitrary file upload vulnerability that allows attackers to upload executable files by bypassing extension validation in the save_attachments function exposed through the Advanced Reviews feature. Attackers can exploit the Custom Fonts extension's flawed strpos() substring check by uploading double-extension filenames such as shell.woff2.php, causing the validation to pass on the substring match while the web server executes the file as PHP, achieving remote code execution. | 9.8 | More Details |
| CVE-2026-51599 | An insufficient input validation vulnerability in the RTSP service of MERCURY MIPC252W v1.0.5 Build 230306 Rel.79931n allows an unauthenticated remote attacker to render an individual TCP connection temporarily unusable via sending an RTSP request with a Content-Length header but no corresponding message body. The affected RTSP parser enters a body-waiting state instead of rejecting the malformed request, causing all subsequent data on the connection to be silently consumed as body content until a server-side timeout closes the connection. | 9.8 | More Details |
| CVE-2026-8307 | Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Webbeyaz Web Design Mediküm Web allows SQL Injection. This issue affects Mediküm Web: through 08072026. NOTE: The vendor was contacted and it was learned that the product is not supported. | 9.8 | More Details |
| CVE-2026-14894 | The Super Forms – Drag & Drop Form Builder plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 6.3.313 via the submit_form function. This is due to missing file type validation and the absence of any capability check on the submit_form nopriv AJAX handler, whose only barrier is a session nonce freely obtainable by unauthenticated visitors via a separate nopriv endpoint. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible. The nonce requirement is trivially bypassed because the super_create_nonce nopriv AJAX action allows any unauthenticated visitor to mint a valid sf_nonce and session cookie in a single prior request, reducing exploitation to two unauthenticated HTTP requests. | 9.8 | More Details |
| CVE-2026-15282 | The Instant Appointment plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'insapp_upload_image_as_attachment' function in all versions up to, and including, 1.2. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. | 9.8 | More Details |
| CVE-2026- | Imager versions before 1.033 for Perl treat unsigned EXIF IFD entry counts as signed. Imager mishandled large EXIF IFD entry count values, treating them as negative numbers. This could lead to an attempt to allocate a block nearly the size of the | 9.8 | More Details |

| | | | |
|---|---|---|---|
| 14454 | address space, which fails and kills the process. An attacker could craft an image with EXIF data that terminates a worker process. | | |
| CVE-2026-28564 | Insufficient Session Expiration, Authentication Bypass by Capture-replay vulnerability in Apache IoTDB. REST Basic Authentication Accepts Stale Cached Credentials This issue affects Apache IoTDB: from 1.0.0 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue. | 9.8 | More Details |
| CVE-2026-58123 | Hermes WebUI before 0.51.788 contains an unauthenticated remote code execution vulnerability that allows remote attackers to execute arbitrary shell commands by accessing the embedded terminal API endpoints without credentials. Attackers can create a session, attach a PTY shell, and write arbitrary commands through the terminal input endpoint to achieve full command execution as the server process user via four sequential unauthenticated HTTP requests. | 9.8 | More Details |
| CVE-2026-12153 | The WP Learn Manager plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.1.8. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to install and activate arbitrary plugins from the WordPress.org repository on the vulnerable site. | 9.8 | More Details |
| CVE-2026-56765 | Vikunja before 2.2.1 contains an authorization flaw where the LinkSharing.ReadAll endpoint exposes share hashes to users with read access, enabling permission escalation to admin-level shares. The GetTaskAttachment endpoint performs permission checks against user-supplied task IDs but fetches attachments by sequential ID without verifying ownership, allowing attackers to download and delete all file attachments across all projects instance-wide. | 9.8 | More Details |
| CVE-2026-5801 | Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Semtek Informatics Software Consulting Trade Ltd. Co. SEM-PMP allows Command Line Execution through SQL Injection. This issue affects SEM-PMP: through 23042026. | 9.8 | More Details |
| CVE-2026-2397 | Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Adam Retail Automation Ltd. MobilMen 20T allows SQL Injection. This issue affects MobilMen 20T: from v3 through 10072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 9.8 | More Details |
| CVE-2026-40008 | Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') vulnerability in Apache IoTDB. The pipe processor reads a fully qualified Java class name and instantiates it using Class.forName().newInstance() without any validation or allowlisting. This issue affects Apache IoTDB: from 1.0.0 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue. | 9.8 | More Details |
| CVE-2026-9701 | The Eventer plugin for WordPress is vulnerable to an insecure password reset mechanism in all versions up to, and including, 4.4.2. The plugin stores a plaintext copy of the password reset key in the `eventer_verification_code` user meta field when a user requests a password reset. The plaintext key stored in `wp_usermeta` can be used with the plugin's custom reset action to set a new password for any user. Combined with another vulnerability such as SQL Injection (CVE-2026-9700), this makes it possible for unauthenticated attackers to extract the plaintext reset key and take over any user account, including administrators. Note: The password reset function only works up to PHP version 7.4. | 9.8 | More Details |
| CVE-2026-52200 | An issue in Generic OEM UZ801_v2.1 4G LTE Router V3.4.3 allows a remote attacker to execute arbitrary code via the /ajax web management API endpoint in MifiService.apk | 9.8 | More Details |
| CVE-2026-55008 | Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network. | 9.6 | More Details |
| CVE-2026-14453 | This vulnerability is a critical Server-Side Template Injection (SSTI) in Centreon's centreon-open-tickets module that leads to Remote Code Execution. The message_confirm field is stored without sanitization and rendered via Smarty with no security policy enabled, allowing any authenticated user, to inject and execute arbitrary code on the server. This results in disclosure of environment secrets and could impact platform availability of Centreon Infra Monitoring product. | 9.6 | More Details |
| CVE-2026-15113 | Use after free in Autofill in Google Chrome on Android prior to 150.0.7871.115 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) | 9.6 | More Details |
| CVE-2026-11563 | The Word Count and Social Shares WordPress plugin through 1.0 does not validate a user-supplied file path before deletion, nor does it have proper authorization or CSRF checks, allowing any authenticated user, such as a Subscriber, to delete arbitrary files on the server, which can lead to a full site takeover (e.g. by deleting wp-config.php). | 9.6 | More Details |
| CVE-2026-59151 | Prowler is a cloud security platform. Prior to 5.30.3, Prowler's SAML authentication flow trusted the email domain asserted in a SAMLResponse when deciding which tenant should receive the final token, and the ACS finish logic in api/src/backend/api/v1/views.py recalculated the tenant from user.email instead of binding token issuance to the validated SAML configuration. An authenticated attacker with a controlled SAML IdP could complete a valid SAML flow for an attacker-controlled domain while asserting an email address from another configured domain, causing a SAMLToken and tenant-scoped JWT to be issued for the wrong tenant and enabling cross-tenant account takeover. This issue is fixed in version 5.30.3. | 9.6 | More Details |
| CVE-2026-50380 | Heap-based buffer overflow in Windows GDI+ allows an unauthorized attacker to execute code over a network. | 9.6 | More Details |
| CVE-2026-15062 | SQL injection vulnerabilities in the Snowflake Snowpark Python SDK (snowpark-python) versions prior to 1.53.0 could allow authenticated low-privilege users to execute SQL beyond their authorization scope. An attacker could exploit these vulnerabilities by embedding SQL payloads in source database column names to escalate privileges via the DataFrameReader.dbapi() API by supplying a specially crafted location parameter to DataFrameWriter write methods to redirect a COPY INTO to an arbitrary source query, or by including a backslash-single-quote sequence in an export path to defeat the normalize_path() sanitizer and inject SQL via DataFrame.to_csv(). Successful exploitation may result in source database compromise, unauthorized cross-tenant data exfiltration, or unauthorized read of Snowflake account data. | 9.6 | More Details |
| CVE-2026-48561 | Improper neutralization of special elements used in a command ('command injection') in Microsoft Copilot allows an unauthorized attacker to execute code over a network. | 9.6 | More Details |
| CVE-2026-13461 | When coupled with the SSL bypass vulnerability, JavaScript can be injected into a WebView in the PayRange version 7.0.7 app. The injection of specific JavaScript function calls allows the attacker to escape the WebView sandbox and perform a number of dangerous actions on the user's device. | 9.6 | More Details |
| CVE-2026-59891 | sigstore-js provides JavaScript libraries for interacting with Sigstore services. Prior to 0.7.1, getRegistryCredentials() reads credentials from the Docker config file and selects an entry by checking whether any configured auth key contains the target registry string. Because this is a substring match rather than an exact host match, credentials configured for one registry can be selected for and transmitted to a different registry whose hostname has a substring relationship with a configured auth key. | 9.6 | More Details |

| | | | |
|---|---|---|---|
| | This issue is fixed in version 0.7.1. | | |
| CVE-2026-59792 | In JetBrains IntelliJ IDEA before 2026.1.4, 2026.2 code execution via path traversal in project workspace ID handling was possible | 9.6 | More Details |
| CVE-2026-57739 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AcyMailing Newsletter Team AcyMailing SMTP Newsletter acymailing allows Blind SQL Injection.This issue affects AcyMailing SMTP Newsletter: from n/a through <= 10.11.0. | 9.3 | More Details |
| CVE-2026-2342 | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in OceanicSoft Informatics Systems Ltd. ValeApp allows Stored XSS. This issue affects ValeApp: through 09072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. | 9.3 | More Details |
| CVE-2026-57707 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in quantumcloud Simple Business Directory Pro simple-business-directory-pro allows SQL Injection.This issue affects Simple Business Directory Pro: from n/a through <= 15.9.4. | 9.3 | More Details |
| CVE-2026-47646 | Improper neutralization of input during web page generation ('cross-site scripting') in Dynamics 365 Customer Voice allows an unauthorized attacker to perform spoofing over a network. | 9.3 | More Details |
| CVE-2026-15378 | A flaw was found in the `guardrails-detectors` component. This vulnerability allows a remote attacker to perform a blind Server-Side Request Forgery (SSRF) by submitting a specially crafted XML Schema Definition (XSD) string. This can lead to unauthorized access to sensitive information, including credentials from cloud metadata services, Kubernetes API, internal MinIO, and other internal network endpoints. Additionally, it enables local file reads of critical data such as service account tokens and pod secrets. | 9.3 | More Details |
| CVE-2026-55879 | OpenReplay is a self-hosted session replay suite. From 1.24.0 before 1.25.0, the OpenReplay tracking SDK accepts custom event names and captured page URLs from any visitor using a public project key, stores them in ClickHouse without output encoding, and later renders them in the authenticated dashboard through TextEllipsis and the event-details modal, allowing an unauthenticated attacker to store script that executes in the dashboard origin, reads the session JWT from localStorage, and takes over a dashboard account. This issue is fixed in version 1.25.0. | 9.3 | More Details |
| CVE-2026-49798 | Use after free in Windows Kernel allows an unauthorized attacker to elevate privileges locally. | 9.3 | More Details |
| CVE-2026-57714 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LatePoint LatePoint latepoint allows Blind SQL Injection.This issue affects LatePoint: from n/a through <= 5.6.3. | 9.3 | More Details |
| CVE-2026-57702 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Melograno Venture Studio Amelia ameliabooking allows Blind SQL Injection.This issue affects Amelia: from n/a through <= 2.4.2. | 9.3 | More Details |
| CVE-2026-15143 | A flaw was found in the file_type content detector of guardrails-detectors. This vulnerability allows a remote attacker to supply an arbitrary XML Schema Definition (XSD) string, which is processed without proper restrictions. This can lead to server-side requests to arbitrary URLs or local file reads, potentially resulting in sensitive information disclosure, such as cloud provider credentials or access to internal network services. | 9.3 | More Details |
| CVE-2026-59515 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Sergey AIWU ai-copilot-content-generator allows Blind SQL Injection.This issue affects AIWU: from n/a through <= 1.5.4. | 9.3 | More Details |
| CVE-2026-57726 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeum Kirki kirki allows Blind SQL Injection.This issue affects Kirki: from n/a through <= 6.0.12. | 9.3 | More Details |
| CVE-2026-59702 | repomix contains a server-side request forgery vulnerability in the POST /api/pack endpoint that allows unauthenticated attackers to make arbitrary outbound requests. The endpoint fails to properly validate http://, https://, and file:// URLs before passing them to git clone, enabling attackers to access private network addresses, GCP metadata services, or local filesystem paths. | 9.3 | More Details |
| CVE-2026-41042 | Unauthenticated callers can supply a malicious H2 JDBC URL through the testConnection API, which executes arbitrary Java code on the server via H2's INIT parameter. Vulnerability in Apache Gravitino. This issue affects Apache Gravitino: before 1.2.1. Users are recommended to upgrade to version 1.2.1, which fixes the issue. This issue only happens when using H2, and H2 is mainly used for testing and local development. Also, Gravitino is typically deployed in the internal environment, so the severity is low. | 9.1 | More Details |
| CVE-2026-58319 | Certain Apache Doris FE HTTP REST administrative APIs were accessible without proper authentication. An unauthenticated attacker with network access to the FE HTTP service could perform unauthorized administrative operations, potentially affecting cluster integrity and availability and leading to cluster instability or denial of service. This issue affects Apache Doris versions prior to 3.1.0. Users are advised to upgrade to Apache Doris 3.1.0 or later. | 9.1 | More Details |
| CVE-2026-27690 | Due to an HTTP Request Smuggling vulnerability in SAP Approuter, an unauthenticated attacker could send a specially crafted HTTP request that leads to request-response desynchronization. This could result in the exposure of user responses and cause the system to become unavailable. This leads to a high impact on confidentiality and availability. | 9.1 | More Details |
| CVE-2026-15265 | A path traversal vulnerability in Tenable Agent 11.2.0 and 11.1.3 and lower allows a privileged attacker to write arbitrary files outside the intended plugin directory, potentially leading to remote code execution. | 9.1 | More Details |
| CVE-2026-9074 | IBM API Connect 10.0.8.0 through 10.0.8.9 and 12.1.0.0 through 12.1.0.3 contains an unauthenticated SQL injection vulnerability in the password reset functionality. | 9.1 | More Details |
| CVE-2026-3014 | Milestone has released a new version of XProtect® (and several cumulative patch updates) which fix security vulnerability in Management Server API.  The vulnerability causes users with edit permissions to the Management Server to be able to execute arbitrary code in context of the Management Server Service. | 9.1 | More Details |
| CVE-2026-59084 | Insufficient Technical Documentation vulnerability in Apache Tomcat since the requirements to securely configure the EncryptInterceptor were not clearly documented. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.23, from 10.1.0-M1 through 10.1.56, from 9.0.13 through 9.0.119, from 8.5.38 through 8.5.100, from 7.0.100 through 7.0.109. Other versions that have reached end of support may also be affected. Users are recommended to upgrade to version 11.0.24, 10.1.57 or 9.0.120 which fix the issue. | 9.1 | More Details |
| | Improper Handling of URL Encoding (Hex Encoding) vulnerability in Apache Tomcat's rewrite valve allowed security constraint | | |

| | | | |
|---|---|---|---|
| CVE-2026-59083 | bypass for some configurations. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.23, from 10.1.0-M1 through 10.1.56, from 9.0.0.M1 through 9.0.119, from 8.5.0 through 8.5.100. Other versions that have reached end of support may also be affected. Users are recommended to upgrade to version 11.0.24, 10.1.57 or 9.0.120, which fix the issue. | 9.1 | More Details |
| CVE-2026-54061 | Dgraph is an open source distributed GraphQL database. Prior to version 25.3.5, Dgraph Alpha exposes the RPCs used for external snapshot import on the public gRPC port `:9080` without authentication or authorization. As a result, an unauthenticated network client can open `StreamExtSnapshot` and send Badger stream data to the target group's store. In addition, the receiver calls `Prepare()` before processing the stream. This operation deletes and replaces the existing DB data. Version 25.3.5 patches the issue. | 9.1 | More Details |
| CVE-2026-44761 | SAP Commerce Cloud could retain a sample OAuth2 client with publicly documented sample credentials originating from sample configuration provided in SAP Help Portal documentation. If left unchanged, an unauthenticated attacker could use these well-known credentials to obtain a valid access token and invoke certain APIs to read and modify data. Successful exploitation results in high impact on confidentiality and integrity, with no impact on availability. | 9.1 | More Details |
| CVE-2026-57158 | FreeRDP is a free implementation of the Remote Desktop Protocol. From 3.21.0 before 3.28.0, FreeRDP clients using the GFX pipeline contain an incomplete fix for CVE-2026-23530 in planar_decompress_plane_rle_only in libfreerdp/codec/planar.c, allowing a malicious RDP server to send a truncated RDPGFX_CMDID_WIRETOSURFACE_1 planar payload that reads one byte past the input buffer. This issue is fixed in version 3.28.0. | 9.1 | More Details |
| CVE-2026-58102 | Crypt::OpenSSL::X509 versions before 2.1.3 for Perl allow a heap out-of-bounds read via a long certificate extension OID in hv_exts. When building the extension hash (via extensions(), extensions_by_long_name(), extensions_by_oid(), or has_extension_oid()), the code passes OBJ_obj2txt()'s return value as the hash-key length; because that value is the OID's full text length rather than the bytes written to the fixed-size buffer (129 bytes), an OID whose text is longer than the 129-byte buffer causes a read past the allocation, exposing adjacent heap memory as the returned hash key. extensions_by_name() uses the static shortname path and is not affected. | 9.1 | More Details |
| CVE-2026-59826 | Metabase is an open-source business intelligence and embedded analytics tool. From 1.55.0 until 1.58.15.1, 1.59.12, 1.60.6.3, and 1.61.2, Metabase did not validate unsafe H2 connection properties on one database-creation code path, allowing an authenticated administrator to register a crafted H2 database connection and execute arbitrary Java code on the Metabase server. This issue is fixed in versions 1.58.15.1, 1.59.12, 1.60.6.3, and 1.61.2. | 9.1 | More Details |
| CVE-2026-51119 | An issue in Invixium IXM WEB v.2.3.85.25 allows an attacker to escalate privileges via the /SystemUsers/CreateAppUser components | 9.1 | More Details |
| CVE-2026-61444 | PraisonAI versions before 4.6.78 contain a code injection vulnerability in deploy/api.py where the agents_file parameter is directly interpolated into an f-string without sanitization. Attackers can inject arbitrary Python code that executes when the generated server code runs via subprocess.Popen(). | 9.1 | More Details |
| CVE-2026-15089 | vulnerability in Drupal Commerce guest registration allows . This issue affects Commerce guest registration versions: *.*. | 9.1 | More Details |
| CVE-2026-56688 | Dell PowerFlex Manager, Version prior to 5.1.0.1, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability during OS Repository processing to achieve arbitrary command execution as root, potentially leading to full appliance compromise and lateral movement into managed infrastructure. | 9.1 | More Details |
| CVE-2026-14487 | The Simple Coherent Form plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the removeUploadDir function in all versions up to, and including, 2.4.13. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). The scf_get_id_upload endpoint freely issues a valid scf_upload_file_removal nonce to any unauthenticated visitor, and the removal endpoint's secondary hash check is forgeable offline because it relies on a hardcoded salt embedded in the plugin source, meaning neither control presents a real authorization boundary. | 9.1 | More Details |
| CVE-2026-40005 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache IoTDB. An attacker can write arbitrary files anywhere the IoTDB process has write permissions with unsafe API. This issue affects Apache IoTDB: from 1.0.0 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue. | 9.1 | More Details |
| CVE-2026-11964 | The User Registration & Membership WordPress plugin before 5.2.2 does not verify the authenticity of incoming payment-provider webhook notifications before acting on them, allowing unauthenticated attackers to forge a payment-approved event and activate a paid membership subscription without completing a real payment. | 9.1 | More Details |
| CVE-2026-15300 | The GEO my WP plugin for WordPress was vulnerable to SQL Injection via the 'distance', 'lat', and 'lng' parameters in versions up to, and including, 4.5.4. The values were read from $_SERVER['QUERY_STRING'] via parse_str() (bypassing wp_magic_quotes, which does not cover $_SERVER), then passed through bare esc_sql() before being interpolated into unquoted numeric positions in the proximity-search query (HAVING/SELECT clause distance math, BETWEEN bounding-box pre-filter) built by gmw_locations_query() in plugins/posts-locator/includes/class-gmw-wp-query.php. Because esc_sql() only escapes string delimiters and these positions are numeric, payloads such as `1 OR SLEEP(3)` survived sanitization. Fixed in 4.5.5 by adding an upstream is_numeric() guard that short-circuits the WHERE clause to `AND 1 = 0` when either coordinate is non-numeric, and by replacing the three esc_sql() calls with (float) casts. | 9.1 | More Details |
| CVE-2026-57830 | The Joomla extension Helix Ultimate is vulnerable to an unauthenticated arbitrary file deletion. | 9.1 | More Details |
| CVE-2026-41041 | URL path injection via unencoded user-supplied identifiers vulnerability in Apache Gravitino. This issue affects Apache Gravitino: from 1.0.0 before 1.2.1. Users are recommended to upgrade to version 1.2.1, which fixes the issue. | 9.1 | More Details |
| CVE-2026-58122 | Hermes WebUI before 0.51.307 contains an authentication bypass vulnerability that allows unauthenticated remote attackers to circumvent local-origin IP restrictions on onboarding endpoints by supplying a spoofed X-Forwarded-For header with a loopback address. Attackers can exploit this bypass to perform server-side request forgery against internal services including cloud metadata endpoints, overwrite LLM provider configuration and API keys with attacker-controlled values, or initiate OAuth device-code flows to obtain persistent access tokens stored in auth.json. | 9.1 | More Details |
| CVE-2026-51597 | MERCURY MIPC252W IP camera v1.0.5 Build 230306 Rel.79931n does not implement nonce expiration in RTSP Digest authentication. An adjacent network attacker can capture a legitimate authentication exchange and replay the nonce and response values in a new connection to bypass authentication without knowledge of the device credentials, gaining unauthorized access to the live video stream. | 9.1 | More Details |

| | | | |
|---|---|---|---|
| CVE-2026-62327 | 9Router through version 0.4.41 contains an unauthenticated information disclosure vulnerability that allows remote attackers to retrieve plaintext API keys for all connected AI provider accounts by sending a single unauthenticated request to the /api/usage/stats endpoint. Attackers can exploit the missing authentication middleware on the Next.js API route to obtain full API key strings alongside token counts, cost breakdowns, and request metadata, enabling unauthorized use of connected AI provider accounts, billing fraud, and quota exhaustion. | 9.1 | More Details |
| CVE-2026-14261 | A vulnerability in the Xerte Online Tools allows for authentication bypass and remote code execution via reinstallation through the /setup/ folder, enabling attackers to reinstall the service to a remote database they control. | 9.1 | More Details |
| CVE-2026-40468 | Integer overflow vulnerability has been found in "builtin.c" program file of gawk. This issue may lead to memory exhaustion on the hosting operating system and could be used to overwrite gawk heap metadata and objects with attacker-controlled bytes. It affects gawk in versions 5.4.0 and below. | 9.1 | More Details |
| CVE-2026-40469 | Integer overflow vulnerability has been found in "builtin.c" program file of gawk (do_sub() routine). This issue could be used to overwrite gawk heap metadata and objects causing the program to crash. It affects 32-bit builds of gawk in versions 5.4.0 and below. | 9.1 | More Details |
| CVE-2026-13221 | Perl versions through 5.43.9 produce silently incorrect regular expression matches when an alternation of more than 65535 fixed string branches is compiled into a trie in Perl_study_chunk. When such branches are combined into a trie, the delta between the first branch and the shared tail is stored in a 16-bit field. A branch count above 65535 overflows the field, and the trie's match decision table is truncated with no warning or error. A pattern of this shape produces false positive matches (matching strings it should not) and false negative matches (failing to match strings it should). When such a pattern gates an access or filtering decision, the result is wrong. | 9.1 | More Details |
| CVE-2026-58409 | ChurchCRM is an open-source church management system. Prior to version 7.4.0, an authenticated administrator can achieve Remote Code Execution (RCE) on the server by installing a malicious plugin ZIP archive containing a PHP webshell. The application explicitly includes 'php' in its ALLOWED_EXTENSIONS list, while the dangerous extensions denylist (DENIED_EXTENSIONS) fails to block standard .php files. Because `php` is explicitly included in the allowed extension list for plugin archives, and extracted files are placed directly under the web root, any PHP file inside the ZIP becomes immediately executable via HTTP — without even needing to "enable" the plugin through the application UI. The /plugins/install-url API route (management.php) allows an administrator to source the malicious ZIP from any attacker-controlled HTTPS URL, validating it only against an attacker-supplied SHA-256 hash. This issue has been fixed in version 7.4.0. | 9.1 | More Details |
| CVE-2026-51536 | In OpENer 2.3.0 (commit 76b95cf) when parsing incoming CIP (Common Industrial Protocol) network packets, the length parameter is inconsistently typed across the call stack. Specifically, an upstream length calculated as an int is passed to a downstream function that expects an EipInt16 (a 16-bit signed integer). If a maliciously crafted packet with specific length fields is processed, the length parameter can overflow or be truncated into a negative value. This negative length bypasses subsequent bounds checking (due to signed/unsigned comparison issues) and is ultimately used in memory operations, leading to a Stack Buffer Overflow when reading data in DecodePaddedEPath. | 9.1 | More Details |
| CVE-2026-51537 | EIPStackGroup OpENer 2.3.0 (commit 76b95cf) has an out-of-bounds read issue in Connection Manager handling of ForwardOpen requests when processing short malformed packets. An attacker can send a valid ENIP outer frame carrying a malformed CIP ForwardOpen/LargeForwardOpen request, causing the parser to continue reading fields even when request data is insufficient. This issue is remotely triggerable via network traffic and does not require authentication. | 9.1 | More Details |
| CVE-2026-51538 | EIPStackGroup OpENer 2.3.0 (commit 76b95cf) suffers from an Incorrect Access Control vulnerability in its handling of encapsulation sessions. When the server processes critical encapsulation commands, it verifies whether the provided session_handle exists in the global session list, but it fails to verify whether that handle belongs to the specific TCP connection issuing the request. Because there is no strong binding between a session handle and its originating socket, any attacker on the network can use a valid session handle created by another legitimate client to bypass access controls. | 9.1 | More Details |
| CVE-2026-51541 | OpENer 2.3.0 (commit 76b95cf) has an out-of-bounds read issue in CIP message parsing when handling malformed explicit requests with a forged EPath size. An attacker can send a valid ENIP SendRRData frame carrying a very short CIP payload whose path_size field claims that many more path words are present than are actually available. Because the parser trusts the attacker-controlled path_size and continues decoding path segments without a remaining-length boundary, it reads beyond the end of the stack receive buffer. | 9.1 | More Details |
| CVE-2026-47826 | The blobs.yml path key traversal vulnerability in the BOSH CLI tool allows an attacker to write arbitrary files and exfiltrate sensitive information. Affected versions: BOSH CLI tool versions prior to v7.10.4. | 9.1 | More Details |
| CVE-2026-56260 | Crawl4AI before 0.8.7 contains an arbitrary file write vulnerability in the Docker API server's /screenshot and /pdf endpoints. The output_path parameter accepts arbitrary filesystem paths without validation, allowing an attacker to supply absolute or path-traversal values to write to any location writable by the application's user, overwriting server files and causing denial of service. | 9.1 | More Details |
| CVE-2026-57898 | In Eclipse BaSyx Java Server SDK versions 2.0.0-milestone-05 to 2.0.0-milestone-12, deployments using the MongoDB backend are vulnerable to an unauthenticated arbitrary file write through the AAS thumbnail API. The AAS thumbnail upload path accepted a client-controlled fileName request parameter and passed it through repository file handling as both a repository key and, during thumbnail retrieval, a local filesystem path. With the MongoDB file repository, the supplied filename was treated as an opaque GridFS key and was not normalized or restricted as a filesystem path. A remote attacker could upload thumbnail content using an absolute or traversal-style filename, then trigger thumbnail retrieval so that the uploaded bytes were written to the attacker-chosen path on the server filesystem. This could allow writing files anywhere the Java process has permission to write and may lead to remote code execution. The default InMemory backend is not affected by this specific path because it normalizes and restricts file paths to its temporary directory. The issue is fixed in Eclipse BaSyx Java Server SDK 2.0.0-milestone-13. | 9.0 | More Details |

## OTHER VULNERABILITIES

| CVE Number | Description |
|---|---|
| CVE-2026-15416 | A flaw was identified in Argo CD, the GitOps engine used by Red Hat OpenShift GitOps, that could allow an unauthenticated attacker with network access to the Argo CD repo-server to achieve remote code execution. Under certain conditions, the attacker may then manipulate cached data to deploy malicious Kubernetes resources to managed clusters, potentially resulting in complete cluster compromise. |
| CVE-2026- | Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges over a |

| | |
|---|---|
| 47295 | network. |
| CVE-2026-57969 | Missing authentication for critical function in Azure CycleCloud allows an authorized attacker to elevate privileges over a network. |
| CVE-2025-6784 | The Code Engine plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 0.3.5 via the 'code-engine' shortcode. This is due to the plugin not restricting access to the code injecting functionality of the plugin. This makes it possible for authenticated attackers, with Contributor-level access and above, to execute code on the server. |
| CVE-2026-57786 | Cross-Site Request Forgery (CSRF) vulnerability in purethemes WorkScout-Core workscout-core allows Authentication Bypass.This issue affects WorkScout-Core: from n/a through <= 1.7.08. |
| CVE-2026-59257 | n8n before 1.123.61, 2.x before 2.27.4, and 2.28.x before 2.28.1 contains a SQL injection vulnerability in the legacy MySQL v1 node's executeQuery operation. The operation substitutes evaluated {{ ... }} expression values directly into the raw SQL string without parameterization. When a workflow uses this operation with expression-sourced values and is connected to an externally-reachable trigger (such as a Webhook node), attacker-controlled input reaching those expressions results in SQL injection, allowing execution of arbitrary SQL with the configured MySQL credentials' privileges. The MySQL v2 node, which uses parameterized queries, is not affected. |
| CVE-2026-50398 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Media allows an authorized attacker to elevate privileges over a network. |
| CVE-2026-49795 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally. |
| CVE-2026-58143 | Cotonti Siena 0.9.26 and earlier contains a cross-site request forgery vulnerability that allows unauthenticated attackers to modify administrator configuration by tricking a logged-in administrator into submitting a forged POST request to the admin.php config update handler, which never invokes the application's CSRF validation function. Attackers can disable the PFS module's file extension whitelist by setting pfsfilecheck to 0, enabling any user with PFS access to upload and execute arbitrary PHP files on the server. |
| CVE-2026-2354 | The Swiss Toolkit For WP plugin for WordPress is vulnerable to arbitrary file upload due to a flawed file type validation bypass in the `upload_extension_files()` function in all versions up to, and including, 1.4.6. The `upload_extension_files()` function hooks into WordPress's `wp_check_filetype_and_ext` filter and uses `strpos()` to check if a filename contains a configured extension string, rather than verifying the actual file extension. This makes it possible for authenticated attackers, with Author-level access and above, to upload arbitrary files (including PHP) on the affected site's server which may make remote code execution possible, granted the "Enhanced Multi-Format Image Support" feature is enabled with at least one extension (e.g., avif) in the allowed formats. |
| CVE-2026-58608 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Print Spooler Components allows an authorized attacker to execute code over a network. |
| CVE-2026-14262 | The Simple JWT Login – Allows you to use JWT on REST endpoints. plugin for WordPress is vulnerable to Authentication Bypass to Privilege Escalation in all versions up to, and including, 3.6.6 via the `payload` parameter. The vulnerability exists because `AuthenticateService::generatePayload()` only overwrites JWT payload keys whose names appear in the admin-configured `jwt_payload` list — leaving any attacker-supplied identity claims such as `email`, `id`, or `username` intact and signed into the JWT with the site's HS256 secret. This makes it possible for authenticated attackers, with subscriber-level access and above, to escalate their privileges to that of an Administrator by injecting a target administrator's email address into the `payload` parameter at the `/wp-json/simple-jwt-login/v1/auth` endpoint, then redeeming the resulting JWT at the `/autologin` endpoint to obtain a fully authenticated session as that administrator. |
| CVE-2026-57410 | Incorrect Privilege Assignment vulnerability in MailerPress Team MailerPress mailerpress allows Privilege Escalation.This issue affects MailerPress: from n/a through <= 2.0.2. |
| CVE-2026-15067 | Snowflake Terraform Provider versions prior to 2.18.0 contain several security vulnerabilities, including SQL injection via an unsanitized data source input could result in arbitrary SQL execution under the provider's privileged Snowflake session, potentially enabling sensitive data exfiltration and minting of long-lived access credentials. Exploitation requires the ability for an attacker to influence a workspace variable in a pipeline where this data source was enabled. Improper neutralization of identifier content in user resource inputs could allow DDL injection into user management statements, potentially causing accounts to be created with attacker-controlled credentials and without the security controls configured by the operator. The fix is available in Snowflake Terraform Provider version 2.18.0. Users must manually upgrade. |
| CVE-2026-4275 | The Divi Torque Lite – Divi Theme, Divi Builder & Extra Theme plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.2.3. This is due to the use of '__return_true' as the permission_callback for the /install_plugin and /activate_plugin REST API endpoints, which bypasses WordPress's built-in REST API nonce verification. Although the endpoint callbacks contain internal current_user_can() checks, the absence of nonce verification means that a forged cross-site request from a logged-in administrator's browser will pass the capability check via the admin's session cookies. This makes it possible for unauthenticated attackers to install arbitrary plugins from WordPress. |
| CVE-2026-57371 | Deserialization of Untrusted Data vulnerability in denishua WPJAM Basic wpjam-basic allows Object Injection.This issue affects WPJAM Basic: from n/a through <= 7.0. |
| CVE-2026-57215 | RabbitMQ is a messaging and streaming broker. Prior to 3.13.15, 4.0.20, 4.1.11, and 4.2.6, RabbitMQ allows foreign bindings to amq.rabbitmq.reply-to destinations because volatile direct-reply-to queues can be accepted at bind and route time but are missing from Khepri-backed deletion checks, leaving persistent route entries after unbind. This issue is fixed in versions 3.13.15, 4.0.20, 4.1.11, and 4.2.6. |
| CVE-2026-57713 | Deserialization of Untrusted Data vulnerability in Marcus (aka @msykes) Events Manager events-manager allows Object Injection.This issue affects Events Manager: from n/a through <= 7.3.6. |
| CVE-2026-49178 | Heap-based buffer overflow in Active Directory Domain Services allows an authorized attacker to execute code over a network. |
| CVE-2026-55005 | Heap-based buffer overflow in Microsoft Exchange Server allows an authorized attacker to execute code over a network. |
| | |

| | |
|---|---|
| CVE-2026-15133 | Use after free in InterestGroups in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-15544 | A vulnerability was determined in Shibby Tomato up to 1.28.0000. Affected is the function getupsvar of the file www/apcupsd/tomatodata.cgi of the component apcupsd. This manipulation of the argument Field causes stack-based buffer overflow. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. This project is superseded by FreshTomato. |
| CVE-2026-15543 | A vulnerability was found in Tenda CH22 1.0.0.1. This impacts the function formCertListInfo of the file /goform/CertListInfo. The manipulation of the argument Name results in buffer overflow. The attack can be launched remotely. The exploit has been made public and could be used. |
| CVE-2026-47632 | Improper certificate validation in Azure Monitor Agent allows an unauthorized attacker to elevate privileges over an adjacent network. |
| CVE-2026-48564 | Heap-based buffer overflow in Windows DHCP Server allows an authorized attacker to execute code over a network. |
| CVE-2026-61461 | Dify before 1.16.0-rc1 contains a SQL injection vulnerability in the MyScale vector store backend that allows attackers to execute arbitrary SQL by supplying unsanitized search parameters to the search_by_full_text method without escaping or parameterization. Attackers can inject malicious SQL through the search parameters to read, modify, or delete data in the underlying ClickHouse database. |
| CVE-2026-6212 | Authorization bypass through User-Controlled key vulnerability in Teracity Software Technologies Inc. TeraMIS allows Privilege Abuse. This issue affects TeraMIS: from V03.26.01.14 through 30.04.2026. |
| CVE-2026-62194 | OpenClaw versions 2026.5.20 before 2026.6.9 contain a privilege escalation vulnerability in plugin install commands that allows lower-trust callers to execute or persist actions beyond their intended authorization. Attackers can exploit misconfigured input paths or enabled features to escalate privileges and perform unauthorized actions when the feature is reachable. |
| CVE-2026-47828 | During bosh create-env and bosh delete-env, the CLI uploads compiled CPI packages and rendered job templates to the new VM's DAV blobstore over HTTPS without verifying the server certificate, even though a CA certificate for that endpoint is available in the installation manifest. A network attacker can terminate the TLS connection, harvest the Basic-auth credentials, and read the rendered-templates archive containing every bootstrap secret for the new BOSH Director, then replay the credentials against the real VM's agent for root code execution. Affected versions: bosh-cli versions prior to v7.10.4. |
| CVE-2026-62190 | OpenClaw versions before 2026.6.9 contain an authorization bypass vulnerability in the flock wrapper that allows lower-trust callers to execute or persist actions beyond their intended authorization. Attackers can leverage configured input paths to bypass durable exec approval binding and perform unauthorized operations when the affected feature is enabled. |
| CVE-2026-56086 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an Incorrect Authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. |
| CVE-2026-59723 | Cline is an autonomous coding agent as an SDK, IDE extension, or CLI assistant. Prior to 3.0.30, the Cline Hub dashboard server launched by the cline dashboard command accepts WebSocket connections on the /browser endpoint without validating the Origin header, and when ROOM_SECRET is unset for local 127.0.0.1 binds, isAuthorizedBrowserRequest() allows attacker-controlled websites to send desktopCommand frames that read workspace state, mutate MCP and provider settings, and trigger command execution when a provider or model is configured. This issue is fixed in version 3.0.30. |
| CVE-2026-15070 | The Salon Booking System – Free Version plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 10.30.32. This is due to missing or incorrect nonce validation on the setCustomText function. This makes it possible for unauthenticated attackers to inject arbitrary PHP code into the web-accessible translate-constants.php file within the plugin directory, enabling remote code execution on the server via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. sanitize_text_field() is applied to the POST 'value' parameter but does not neutralize the characters — single quotes, parentheses, semicolons, $, and [] — required to break out of the PHP string literal into which the value is interpolated before being written to disk via file_put_contents(). |
| CVE-2026-5523 | The Divi Form Builder plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 5.1.8. This is due to the update_user() function accepting a user ID parameter from form submissions without verifying that the authenticated user has permission to edit that specific user account, and the handle_register_submission() function only checking if any user is logged in rather than validating permissions for the target user. This makes it possible for authenticated attackers, with subscriber-level access and above, to change the email address and password of any user account, including administrators, resulting in complete account takeover. |
| CVE-2026-50413 | Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally. |
| CVE-2026-13353 | The WP Ultimate CSV Importer – WordPress Import & Export for CSV, XML & Excel plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 8.0.1 via the 'MappedFields' parameter. This is due to missing capability checks on the AJAX handlers for install_addon, saveMappedFields, and StartImport, combined with the plugin nonce being exposed to any authenticated user who can load an admin page, allowing a Subscriber to install the Import WooCommerce add-on, persist attacker-controlled PHP expressions in the MappedFields parameter, and trigger evaluation via eval() in ImportHelpers::get_meta_values(). This makes it possible for authenticated attackers, with subscriber-level access and above, to execute code on the server. |
| CVE-2026-13756 | The WP Grid Builder plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.3.3. This is due to missing authorization and meta key validation in the `update()` handler for the `/wp-json/wpgb/v2/metadata` REST endpoint. This makes it possible for authenticated attackers, with Subscriber-level access and above, to elevate their privileges to Administrator by updating their own `wp_capabilities` user meta with a crafted nested array payload. |
| CVE-2026-15129 | Use after free in Views in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) |
| CVE-2026-59734 | Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.469, Coolify's app/Jobs/ApplicationDeploymentJob.php generate_healthcheck_commands() function directly interpolated the health_check_host, health_check_method, and health_check_path parameters into shell commands without proper sanitization, allowing authenticated users to execute arbitrary commands inside deployment containers. This issue is fixed in version 4.0.0-beta.469. |
| CVE- | |

| | |
|---|---|
| 2026-50663 | Relative path traversal in Age of Empires II: Definitive Edition Game allows an unauthorized attacker to execute code over a network. |
| CVE-2026-59260 | OpenWrt luci-app-samba4 read ACL grants file.exec permission on /usr/sbin/smbd, allowing authenticated delegated users to execute the Samba daemon with caller-controlled command-line arguments. Attackers can pass arbitrary Samba global options such as message command to a root smbd process, triggering command execution when SMB protocol messages are processed. |
| CVE-2026-50370 | Heap-based buffer overflow in Windows DHCP Server allows an unauthorized attacker to execute code over an adjacent network. |
| CVE-2026-44795 | Spinnaker is an open source, multi-cloud continuous delivery platform. Prior to 2026.1.0, 2026.0.3, 2025.4.4, and 2025.3.3, unsafe YAML processing bypasses safe deserialization when using CloudFormation deployments or CloudFoundry baking. The use of a non-safe constructor allows arbitrary loading of Java classes, leading to remote code execution. This issue is fixed in versions 2026.1.0, 2026.0.3, 2025.4.4, and 2025.3.3. |
| CVE-2026-61463 | Shiori contains a privilege escalation vulnerability in the account update endpoint that allows authenticated users to modify the owner field without authorization checks. Attackers can escalate to administrator by submitting a crafted PATCH request with owner: true, then re-authenticate to obtain an admin JWT token granting full system access. |
| CVE-2026-50369 | Use after free in Windows Remote Desktop Services allows an authorized attacker to elevate privileges over a network. |
| CVE-2026-58378 | Allwinner H616 TV Box TV98 has ADB enabled and exposed to the network on production. An attacker could request for ADB authorization and gain root level privileges if the victim allows access. |
| CVE-2026-61876 | LuCI versions fail to properly encode DHCPv6 lease hostnames before rendering in status tables, allowing adjacent network attackers to inject HTML markup. Attackers can send a DHCPv6 Client FQDN containing script tags that execute in the administrator's browser when viewing DHCP lease pages. |
| CVE-2026-54982 | Integer underflow (wrap or wraparound) in Reliable Multicast Transport Driver (RMCAST) allows an unauthorized attacker to execute code over an adjacent network. |
| CVE-2026-54107 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K allows an authorized attacker to elevate privileges locally. |
| CVE-2026-60102 | Horde Virtual File System (VFS) API before 3.0.1 contains an OS command injection vulnerability in the Horde_Vfs_Smb driver where the _escapeShellCommand() method fails to sanitize command substitution sequences, allowing authenticated attackers to inject arbitrary shell commands through user-controlled filenames. Attackers can supply malicious filenames containing unescaped command substitution payloads through operations such as file upload, folder creation, rename, or deletion, which are interpolated into a double-quoted shell context and executed via proc_open() through /bin/sh -c before smbclient runs, resulting in arbitrary command execution on the underlying system. |
| CVE-2026-50360 | Incorrect implementation of authentication algorithm in Windows SMB Server allows an authorized attacker to elevate privileges over a network. |
| CVE-2026-54118 | Deserialization of untrusted data in SQL Server allows an authorized attacker to execute code over a network. |
| CVE-2026-54117 | Deserialization of untrusted data in SQL Server allows an authorized attacker to execute code over a network. |
| CVE-2026-61875 | luci-app-upnp contains a stored cross-site scripting vulnerability that allows unauthenticated LAN clients to inject JavaScript via UPnP IGD AddPortMapping SOAP requests. Attackers can send malicious HTML in the NewPortMappingDescription field, which miniupnpd stores and luci-app-upnp renders without output encoding, executing the payload when administrators view the UPnP or Status pages. |
| CVE-2026-13492 | The UsersWP plugin for WordPress is vulnerable to Arbitrary File Deletion in versions up to, and including, 1.2.65. This is due to insufficient validation of file-field values in the UsersWP_Validation::validate_fields() function (which falls through to sanitize_text_field() for fields of type 'file', leaving directory-traversal sequences intact) combined with the UsersWP_Forms::upload_file_remove() AJAX handler building the deletion target from the uploads basedir concatenated with the attacker-controlled metadata value without any realpath canonicalization or uploads-directory boundary check before calling unlink(). This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the affected site's server, including wp-config. |
| CVE-2026-55207 | Pimcore is an Open Source Data & Experience Management Platform. Prior to 2025.4.6 and 2026.1.6, an unauthenticated attacker who knows a valid admin username can take over any Pimcore admin account by sending a password reset request with an attacker-controlled resetPasswordUrl. The server generates a real cryptographic recovery token, appends it to the supplied URL, and emails the link to the victim; when the victim clicks the link, the token is sent to the attacker and can be used with POST /pimcore-studio/api/login/token to authenticate with full admin privileges while bypassing two-factor authentication. This issue is fixed in versions 2025.4.6 and 2026.1.6. |
| CVE-2026-50382 | Untrusted pointer dereference in Windows DirectX allows an authorized attacker to execute code locally. |
| CVE-2026-15480 | A vulnerability was identified in Trendnet TEW-635BRM up to 1.00.03. This affects the function start_httpd of the file /sbin/rc of the component Web Service. Such manipulation of the argument device_name leads to stack-based buffer overflow. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor explains: "We are unable to confirm if the vulnerability exists. This item has been EOL since 2011. We will make an official announcement of possible vulnerabilities, and recommend users to switch devices." This vulnerability only affects products that are no longer supported by the maintainer. |
| CVE-2026-15481 | A security flaw has been discovered in Trendnet TEW-635BRM up to 1.00.03. This vulnerability affects the function ipoa_test of the file /sbin/rc of the component IPoA WAN Connection Setup. Performing a manipulation of the argument ipoa_ipaddr results in command injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The vendor explains: "We are unable to confirm if the vulnerability exists. This item has been EOL since 2011. We will make an official announcement of possible vulnerabilities, and recommend users to switch devices." This vulnerability only affects products that are no longer supported by the maintainer. |

| | |
|---|---|
| CVE-2026-50385 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally. |
| CVE-2026-55773 | CedarJava is an open source Java implementation of the Cedar policy language, used for fine-grained authorization decisions. In versions prior to 2.3.6, 3.4.1 and 4.9.0, under certain circumstances, improper input handling could allow Cedar-expression injection via unescaped toCedarExpr(). The toCedarExpr() method on Cedar Value types does not escape special characters (" or \) when converting values to Cedar source code. If an integrator uses toCedarExpr() to build policy text at runtime from user-controlled values, an actor could inject arbitrary Cedar expressions. For example, injecting \|\| true into a permit ... when { ... } clause could make the permit unconditional, or injecting && false into a forbid clause could prevent the forbid from triggering. This issue requires the integrator to use toCedarExpr() to build policy text at runtime from user-controlled input. This vulnerability has been fixed in versions 2.3.6, 3.4.1, and 4.9.0. |
| CVE-2026-55771 | CedarJava is an open source Java implementation of the Cedar policy language, used for fine-grained authorization decisions. In versions prior to 4.9.0, the EntityIdentifier.equals() has inverted null/self branches which could lead to incorrect equality comparisons. The EntityIdentifier.equals() method has inverted logic for null and self-reference checks, returning true for null comparisons and false for self-comparisons. This does not affect Cedar authorization decisions (computed in Rust from JSON), but could affect integrators who perform their own equality checks on entity identifiers. This issue has been fixed in version 4.9.0. |
| CVE-2026-54999 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows TCP/IP allows an unauthorized attacker to execute code over an adjacent network. |
| CVE-2026-58253 | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.0, 2.12.7, and 2.11.16, when no_auth_user was configured, a parser fast path intended for ordinary client connections could also apply to route or leafnode listeners, allowing an unauthenticated peer to bypass inter-server CONNECT authentication and operate with the privileges associated with that connection type. This issue is fixed in versions 2.14.0, 2.12.7, and 2.11.16. |
| CVE-2026-49970 | Laravel-Mediable before 7.0.0 contains a path traversal vulnerability in the File::sanitizePath() function that allows attackers to write uploaded files to arbitrary locations by controlling the directory argument passed to MediaUploader::toDestination(). Attackers can exploit the permissive character-class regex that allows both dot and slash characters combined with an ineffective trailing trim() call to bypass sanitization and upload files to sensitive locations such as the document root, environment configuration files, or application configuration directories, enabling remote code execution. |
| CVE-2026-50342 | Improper access control in Windows MIDI Service Module allows an authorized attacker to elevate privileges locally. |
| CVE-2026-15483 | A security vulnerability has been detected in TRENDnet TEW-821DAP 1.12B01. Impacted is the function sub_41EC14 of the file /goform/tools_nslookup of the component ssi. The manipulation of the argument nslookup_target leads to buffer overflow. It is possible to initiate the attack remotely. The vendor explains: "We are unable to confirm the existence of the vulnerabilities for (...) TEW-821DAP (v1.0R) as these items have been EOL. " This vulnerability only affects products that are no longer supported by the maintainer. |
| CVE-2026-15484 | A vulnerability was detected in TRENDnet TEW-821DAP 1.12B01. The affected element is the function sub_41EC14 of the file /goform/tools_nslookup of the component ssi. The manipulation results in buffer overflow. It is possible to launch the attack remotely. The vendor explains: "We are unable to confirm the existence of the vulnerabilities for (...) TEW-821DAP (v1.0R) as these items have been EOL. " This vulnerability only affects products that are no longer supported by the maintainer. |
| CVE-2026-55772 | CedarJava is an open source Java implementation of the Cedar policy language, used for fine-grained authorization decisions. In versions prior to 2.3.6, 3.4.1 and 4.9.0, under certain circumstances, improper input handling could allow Record-to-Entity type confusion across the Java-Rust FFI boundary. CedarJava sends authorization requests to the Rust cedar-policy evaluator as JSON. The JSON protocol reserves magic single-key object shapes (__entity and __extn) for entity references and extension values. When serializing a CedarMap, there is no validation preventing these reserved keys from being used. If an integrating service builds a CedarMap from caller-supplied key/value data (such as request headers, user-defined metadata, or resource tags), an actor who controls those keys could cause the Rust evaluator to interpret a record as an entity reference. This issue requires the integrating service to build a CedarMap where the an actor controls the keys, and a policy must reference that value in a when/unless clause. This vulnerability has been fixed in versions 2.3.6, 3.4.1, and 4.9. |
| CVE-2026-49972 | Laravel-Mediable before 7.0.0 contains a file upload vulnerability that allows unauthenticated attackers to achieve remote code execution by uploading a file with an embedded PHP extension disguised within a double extension such as shell.php.jpg. The PATHINFO_FILENAME extraction preserves the inner .php extension in the base name, and on misconfigured Apache or nginx servers that execute any filename containing .php as PHP, the stored file is interpreted as executable code while all MIME type, extension, and aggregate type validation checks pass due to the outer .jpg extension. |
| CVE-2026-59148 | Mockoon provides way to design and run mock APIs. Prior to 9.7.0, Mockoon's admin API in commons-server/src/libs/server/admin-api.ts is mounted on the same Express listener as user-defined mock routes, enabled by default in shipped runtimes, serves Access-Control-Allow-Origin: * with write methods allowed, and has no authentication. Any unauthenticated caller who can reach the mock server port can read MOCKOON_* environment variables, write arbitrary process environment variables through /mockoon-admin/env-vars, rewrite mock route bodies, statuses, and headers through PUT /mockoon-admin/environment, read transaction logs and SSE streams, and purge state. This issue is fixed in version 9.7.0. |
| CVE-2026-15132 | Uninitialized Use in V8 in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-15155 | The Essential Addons for Elementor – Popular Elementor Templates & Widgets plugin for WordPress is vulnerable to Authenticated Account Takeover via Email Header Injection in all versions up to, and including, 6.6.10 This is due to insufficient server-side validation of a Login/Register widget setting used to construct outgoing email headers — the allowed-values restriction is enforced only in the client-side editor UI and not on the server, and the applied sanitization does not strip or encode CR/LF characters, allowing CRLF sequences stored in that setting to survive into raw mail headers. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject an additional Bcc header into the WordPress administrator's password-reset notification email, receive a copy of a valid administrator password-reset link, and achieve full administrator account takeover. |
| CVE-2026-15545 | A vulnerability was identified in Shibby Tomato up to 1.28.0000. Affected by this vulnerability is the function main of the file www/apcupsd/tomatodata.cgi of the component apcupsd. Such manipulation leads to out-of-bounds write. The attack may be launched remotely. The exploit is publicly available and might be used. This project is superseded by FreshTomato. |
| CVE-2026-14495 | The DoLogin Security plugin for WordPress is vulnerable to Authentication Bypass via Insufficient Randomness in all versions up to, and including, 4.3. The vulnerability exists because `dologin\s::rrand()` seeds the Mersenne Twister with `mt_srand((double) microtime() * 1000000)` — discarding the integer-seconds component of `microtime()` and constraining the seed to a range of approximately 10^6 values (~20 bits of entropy) — after which every character of the 32-character magic-link token is drawn sequentially with `mt_rand()`, making the entire token a deterministic function of that seed. Because `Pswdless::try_login()` is registered on the unauthenticated `init` hook, resolves the target account by the auto-increment numeric ID embedded in the `?dologin=<id>.<hash>` parameter, performs the hash comparison using a non-constant-time `!=` operator, and then calls `wp_set_auth_cookie()` directly — never passing through `wp_authenticate()` and therefore never triggering the plugin's own `Auth::_has_login_err()` lockout — an unauthenticated attacker can brute-force the ~10^6-candidate seed space to reconstruct an active passwordless login token and authenticate as any targeted user, including administrators, without a password. Exploitation requires that a valid, unexpired passwordless login link (active for up to 7 days) exists for the target account at the time of the attack, and that the |

| | |
|---|---|
| | numeric link ID is known or guessable from the auto-increment primary key. |
| CVE-2026-15121 | Use after free in WebRTC in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-62199 | OpenClaw versions before 2026.6.6 contain a flaw in host exec environment filtering that can miss interpreter startup variables. When the affected feature is enabled and reachable, a lower-trust caller or configured input path can supply crafted environment variables to execute or persist actions beyond the caller's intended authorization. |
| CVE-2026-15695 | A flaw has been found in Tenda BE12 Pro 16.03.66.23. The affected element is the function fromDhcpListClient of the file /goform/DhcpListClient. This manipulation of the argument page causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been published and may be used. |
| CVE-2026-62200 | OpenClaw versions before 2026.6.6 contain a flaw in host exec environment filtering that could allow Git ext transport to be abused. When the affected feature is enabled and reachable, a lower-trust caller or configured input path could execute or persist actions beyond the caller's intended authorization. |
| CVE-2026-15548 | A security vulnerability has been detected in Shibby Tomato up to 1.28.0000. This vulnerability affects the function sub_407220 of the file /usr/sbin/httpd of the component DNS List Rendering. The manipulation leads to stack-based buffer overflow. The attack is possible to be carried out remotely. This project is superseded by FreshTomato. |
| CVE-2026-15110 | Use after free in Extensions in Google Chrome prior to 150.0.7871.115 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High) |
| CVE-2026-50438 | Improper link resolution before file access ('link following') in Microsoft PC Manager allows an authorized attacker to elevate privileges locally. |
| CVE-2026-14489 | The WHMCS Bridge plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the connect() function in all versions up to, and including, 6.9. This makes it possible for authenticated attackers, with Custom-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. |
| CVE-2025-30007 | HestiaCP before 1.9.5 contains an authenticated OS command injection vulnerability that allows low-privilege authenticated users to execute arbitrary commands as root by injecting a single-quote character into unvalidated DNS record types. Attackers can exploit insufficient input validation in is_dns_record_format_valid() combined with unsafe eval-based parsing in update_domain_zone() to prematurely close a variable assignment string and achieve full root code execution on the underlying host in a single DNS record creation step. |
| CVE-2026-15694 | A vulnerability was detected in Tenda BE12 Pro 16.03.66.23. Impacted is the function fromSetIpBind of the file /goform/SetIpBind. The manipulation of the argument page results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit is now public and may be used. |
| CVE-2026-57855 | Cockpit CMS contains a missing authorization vulnerability in the Bucket file storage API (/system/buckets/api). The api() method in modules/System/Controller/Buckets.php executes bucket commands (ls, upload, removefiles, rename, createfolder) without performing any ACL or role check. Any authenticated user, regardless of role, can perform all bucket operations on any named bucket, including buckets intended for admin use only. |
| CVE-2026-15112 | Use after free in Ozone in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) |
| CVE-2026-15114 | Out of bounds read and write in Codecs in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to potentially exploit heap corruption via a crafted video file. (Chromium security severity: High) |
| CVE-2026-15116 | Use after free in Actor in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-15696 | A vulnerability has been found in Tenda BE12 Pro 16.03.66.23. The impacted element is the function fromVirtualSer of the file /goform/VirtualSer. Such manipulation of the argument page leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. |
| CVE-2026-54469 | Dell Unisphere for PowerMax, version(s) 10.3.0.5 and prior, contain(s) a Deserialization of Untrusted Data vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. |
| CVE-2026-57856 | Cockpit CMS contains a path traversal vulnerability in the Bucket file storage API (/system/buckets/api). The api() method in modules/System/Controller/Buckets.php sanitizes the bucket name with preg_replace('/[^a-zA-Z0-9-_\\.]/','', $bucket), which permits '..' and '../' sequences. The sanitized value is interpolated into a Flysystem path as uploads://buckets/{bucket}. Flysystem's WhitespacePathNormalizer resolves 'buckets/..' to the empty string (the uploads storage root) without raising PathTraversalDetected because the '..' has a preceding component to consume. An authenticated low-privileged user can send a crafted request with a '../' bucket name to list, upload, and delete files across all buckets, including those belonging to other users or roles |
| CVE-2026-61460 | Krayin CRM through 2.2.3 contains an insecure direct object reference vulnerability in LeadController, PersonController, OrganizationController, QuoteController, and ActivityController that allows authenticated users to edit, update, or delete records owned by other users. Attackers can modify CRM records and reassign ownership by exploiting missing record-level ownership validation in edit, update, and destroy methods. |
| CVE-2026-15123 | Inappropriate implementation in DOM in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-14482 | The 多说社会化评论框 plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.2. The vulnerability exists due to a missing capability and nonce check on a directly web-accessible API endpoint, combined with a trivially forgeable HMAC-SHA1 signature keyed on an always-empty WordPress option, which allows the endpoint's `update_option` handler to pass attacker-controlled `option` and `value` parameters directly to WordPress's `update_option` function without any allowlist or sanitization. This makes it possible for unauthenticated attackers to update arbitrary WordPress options — such as setting `default_role` to `administrator` and enabling open registration — and subsequently register an account with full administrator privileges. |
| CVE- | The Widget Logic Visual plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.52 via the widget_logic_visual_check_visibility function. This is due to missing capability check and nonce verification on the widget-logic-update-conditional-tags AJAX action |

| | |
|---|---|
| 2026-14158 | combined with insufficient sanitization of the 'nwlv[cod-tag]' parameter before storage and subsequent use in an eval() call. This makes it possible for authenticated attackers, with subscriber-level access and above, to execute code on the server. |
| CVE-2026-57828 | The Joomla extension Phoca Downloads is vulnerable to an authenticated arbitrary file upload that allows registered users uploading executable files and leads to full RCE. |
| CVE-2026-10037 | A sandbox escape vulnerability exists in the OpenJDK packages provided in Ubuntu. The .jar MIME handlers installed by these packages execute files marked as executable when the mailcap package is installed. A compromised or malicious sandboxed application with access to the OpenURI portal via xdg-desktop-portal-gtk can write a malicious .jar file to the host file system, set its executable bit, and trigger the handler to execute arbitrary code outside of the sandbox environment. |
| CVE-2026-54149 | MaxKB is an open-source AI assistant for enterprise. Prior to 2.10.0-lts, MaxKB tool import functionality in apps/tools/serializers/tool.py and MCP referencing mode in apps/application/chat_pipeline/step/chat_step/impl/base_chat_step.py do not consistently validate MCP transport type, allowing an authenticated user to import a .tool file containing stdio transport with malicious commands and trigger the configuration through an AI Chat node so MultiServerMCPClient executes arbitrary system commands. This issue is fixed in version 2.10.0-lts. |
| CVE-2026-2398 | Authorization bypass through User-Controlled key vulnerability in Adam Retail Automation Ltd. MobilMen 20T allows Privilege Escalation. This issue affects MobilMen 20T: from v3 through 10072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15126 | Use after free in Forms in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-15125 | Inappropriate implementation in Forms in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-15107 | Use after free in IndexedDB in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium) |
| CVE-2026-61434 | PraisonAI versions before 4.6.78 contain an allowlist bypass vulnerability in shell command execution that allows attackers to execute restricted commands via find's built-in -exec, -execdir, and -delete actions. Attackers can craft find commands with these built-in actions to read blocked files, delete files, or execute non-allowlisted binaries without triggering shell metacharacter filters. |
| CVE-2026-15693 | A security vulnerability has been detected in Tenda BE12 Pro 16.03.66.23. This issue affects the function fromSafeMacFilter of the file /goform/SafeMacFilter. The manipulation of the argument page leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. |
| CVE-2026-15692 | A weakness has been identified in Tenda BE12 Pro 16.03.66.23. This vulnerability affects the function fromSafeUrlFilter of the file /goform/SafeUrlFilter. Executing a manipulation of the argument page can lead to stack-based buffer overflow. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. |
| CVE-2026-15691 | A security flaw has been discovered in Tenda BE12 Pro 16.03.66.23. This affects the function fromSafeClientFilter of the file /goform/SafeClientFilter. Performing a manipulation of the argument page results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. |
| CVE-2026-57386 | Incorrect Privilege Assignment vulnerability in Kodezen LLC aBlocks ablocks allows Privilege Escalation.This issue affects aBlocks: from n/a through < 2.9.1. |
| CVE-2026-1359 | The Genolve – AI image AI video generation plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the genolve_setOpt() function in all versions up to, and including, 5.0.5. This makes it possible for authenticated attackers, with Contributor-level access and above, to update arbitrary WordPress options, including enabling user registration and setting the default role to administrator, resulting in privilege escalation. |
| CVE-2026-59793 | In JetBrains TeamCity before 2026.1.2 arbitrary file access was possible via the Perforce VCS integration |
| CVE-2026-50444 | Missing authentication for critical function in Windows Server Update Service allows an authorized attacker to elevate privileges over a network. |
| CVE-2026-15118 | Use after free in Input in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-55596 | Plate is a rich-text editor with AI and shadcn/ui. From 53.0.0 until 53.1.4, the media embed renderer trusts serialized provider or sourceUrl metadata in useMediaState and skips parseMediaUrl protocol validation, allowing a crafted Plate document to set a known video provider while keeping url as a javascript: iframe source that the registry MediaEmbedElement renders directly as an iframe src when a victim opens the document. This issue is fixed in version 53.1.4. |
| CVE-2026-55466 | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, UploadFileRequest sanitizes SVG content only when PHP finfo reports image/svg+xml and UploadedFilesController serves attachments inline without using StorageHelper::allowSafeInline(), allowing a low-privilege user to upload active XHTML or XML content that is later served same-origin and executes JavaScript in a viewer’s browser. This issue is fixed in version 8.6.2. |
| CVE-2026-6896 | GitLab has remediated an issue in GitLab EE affecting all versions from 13.11 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an authenticated user with developer-role permissions to execute arbitrary scripts in another user's browser session due to improper sanitization of user-supplied input. |
| CVE-2026-14891 | HashiCorp Nomad and Nomad Enterprise are vulnerable to a sandbox escape in the Docker task driver that may allow a job submitter to bind-mount a host path into a container even when volume bind mounts are disabled, potentially leading to reading and writing files on the host. This vulnerability, CVE-2026-14891, is fixed in Nomad Community Edition 2.0.4 and Nomad Enterprise 2.0.4, 1.11.8, and 1.10.14. |
| CVE-2026- | Bitwarden Server before 2026.6.0 does not verify that the email in a POST /auth-requests/admin-request body belongs to the authenticated caller, allowing a low-privileged organization member to obtain another user's vault key and a victim-scoped access token by creating a Trusted Device Encryption authentication request, bound to an attacker-controlled public key, that is readable from an unauthenticated endpoint once approved resulting in disclosure of the victim's vault |

| | |
|---|---|
| 60104 | key and account takeover. |
| CVE-2026-55429 | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, `UpsertWorkspaceApp` overwrites an existing app's `agent_id` on a primary-key conflict and `insertAgentApp` accepts the app ID from the provisioner's `CompleteJob` payload without verifying it belongs to the workspace being built. `CompleteJob` runs under `dbauthz.AsProvisionerd` so the authorization layer does not block the cross-workspace upsert. Exploitation requires elevated access as a template author or external provisioner operator. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 verifies that any existing `workspace_apps` row matching the supplied ID belongs to the workspace being built and rejects cross-workspace agent reassignment. No known workarounds are available. |
| CVE-2026-61462 | mcp-gitlab contains a path traversal vulnerability in the job_id parameter of build/index.js that allows attackers to redirect GitLab API requests to arbitrary endpoints. Attackers can supply crafted job_id values like ../../../user to escape the intended path prefix and access arbitrary GitLab API resources using the operator's personal access token. |
| CVE-2026-56261 | Crawl4AI before 0.8.7 contains a server-side request forgery (SSRF) vulnerability in the Docker API server's /crawl/job and /llm/job endpoints, which accept webhook URLs without destination validation. An attacker can supply webhook URLs pointing to private or internal IP ranges, Docker networks, or cloud metadata endpoints (e.g. 169.254.169.254), causing the server to make requests to internal services and potentially expose cloud metadata. |
| CVE-2026-55638 | 9Router is an AI router & token saver. Prior to 0.5.2, 9router protects /v1, /v1beta, /api/v1, and /api/v1beta in src/dashboardGuard.js but omits /codex before next.config.mjs rewrites /codex/* to /api/v1/responses. A remote unauthenticated attacker can send requests to /codex/* to bypass the API-key gate and cause the server to make upstream provider calls using operator-stored LLM provider credentials. This issue is fixed in version 0.5.2. |
| CVE-2026-55604 | DeepSeek MCP Server is an MCP server for DeepSeek V4. Starting in version 1.4.2 and prior to version 1.7.0, the process-global `SessionStore` accepts caller-supplied `session_id` values without binding them to any authenticated principal or transport session. An attacker can enumerate active session IDs via `deepseek_sessions`, then reuse a victim-controlled `session_id` in `deepseek_chat` to retrieve and continue the victim's conversation context. Version 1.7.0 contains a patch. |
| CVE-2026-52747 | ModSecurity is an open source, cross platform web application firewall (WAF) engine for Apache, IIS and Nginx. Prior to 3.0.16, the multipart/form-data request body parser in libmodsecurity silently removes embedded line breaks from non-file form-field values before exporting them to ARGS and ARGS_POST because src/request_body_processor/multipart.cc overwrites reserved bytes in m_reserve instead of appending the current buffer. This creates a parser differential between ModSecurity and backend applications that preserve line breaks in form fields, allowing rules that inspect ARGS or ARGS_POST to miss payloads whose dangerous syntax depends on a line break. This issue is fixed in version 3.0.16. |
| CVE-2026-59835 | A exposure of resource to wrong sphere vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.2, FortiSandbox 4.4.3 through 4.4.8 may allow an unauthenticated attacker to access the VNC server of VMs performing scanning via network requests. |
| CVE-2026-60105 | Monsta FTP before 2.14.5 contains a server-side request forgery vulnerability in the fetchRemoteFile action caused by an incomplete IP blocklist check in the isBlockedIP() function, which fails to detect embedded IPv4 addresses within IPv4-mapped IPv6 addresses. An unauthenticated attacker can obtain a CSRF token from the public getSystemVars endpoint and submit a fetchRemoteFile request with a source URL resolving to an IPv4-mapped address, causing the server to issue HTTP requests to internal services and write responses to an attacker-controlled FTP destination, enabling retrieval of cloud instance metadata credentials. |
| CVE-2026-62242 | Spring Boot Admin Server before 4.1.2 contains a server-side request forgery vulnerability that allows unauthenticated attackers to register instances with attacker-controlled healthUrl and managementUrl parameters without validation against private IP ranges or metadata endpoints. Attackers can force the server to make HTTP requests to arbitrary internal addresses and retrieve response bodies via the actuator proxy to exfiltrate cloud credentials. |
| CVE-2026-58192 | Appium is a cross-platform automation framework for all kinds of apps, built on top of the W3C WebDriver protocol. Prior to 1.1.6, the Appium storage plugin exposes POST /storage/delete, whose handler passes the user-supplied name value directly into path.join(storageRoot, name) and fs.rimraf() without path sanitization, allowing an unauthenticated remote client to escape the storage root with ../ sequences and recursively delete arbitrary writable files or directories. This issue is fixed in version 1.1.6. |
| CVE-2026-12582 | The Library Management System WordPress plugin before 3.5.8 does not sanitize and escape a user-supplied parameter before using it in a SQL statement, allowing unauthenticated attackers to perform SQL injection and extract arbitrary data from the database, including user password hashes. |
| CVE-2026-57709 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WP Swings Membership For WooCommerce membership-for-woocommerce allows Path Traversal.This issue affects Membership For WooCommerce: from n/a through <= 3.1.0. |
| CVE-2026-61426 | PraisonAI before 1.7.3 contains an insecure default configuration that binds to all interfaces with no API key requirement and wildcard CORS. Unauthenticated attackers can call GET /api/agents to read agent instructions and system prompts, or POST /api/chat to invoke agents without authentication. |
| CVE-2026-57389 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Adrian Tobey Groundhogg groundhogg allows Path Traversal.This issue affects Groundhogg: from n/a through <= 4.4.1. |
| CVE-2026-57810 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Saad Iqbal APIExperts Square for WooCommerce woosquare allows Blind SQL Injection.This issue affects APIExperts Square for WooCommerce: from n/a through <= 4.7.4. |
| CVE-2026-62197 | OpenClaw before 2026.6.6 contains a policy bypass vulnerability in browser CDP discovery that accepts blocked WebSocket URLs. Attackers with lower-trust access can reach network destinations that should have been blocked by OpenClaw policy when the affected feature is enabled. |
| CVE-2026-56002 | A heap bufferflow in pcfReadFont() due to missing glyph bounds checking in libXfont2 before 2.0.8  allows attackers authenticated as X client to execute code within the X server. |
| CVE-2026-57385 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in appsbd Vitepos vitepos-lite allows Blind SQL Injection.This issue affects Vitepos: from n/a through <= 3.4.2. |
| CVE-2026-55789 | Logto is the modern, open-source auth infrastructure for SaaS and AI apps. Prior to 1.41.0, Logto's self-hosted SAML application IdP built the signed SAML response and assertion by string-substituting user-controlled profile attributes such as name, email, and custom attribute-mapping values into element-text placeholders of a SAML XML template using samlify 2.10.0, which left those placeholders unescaped. An authenticated low-privilege user could place XML markup in a profile attribute so Logto signed a forged SAML attribute, such as an arbitrary role, allowing privilege escalation at relying Service Providers that authorize on SAML attributes. This issue is fixed in version 1.41.0. |

| | |
|---|---|
| CVE-2026-61429 | PraisonAI versions before 1.6.78 contain a server-side request forgery vulnerability in the Crawl4AI/Chromium backend that allows attackers to bypass SSRF validation by exploiting DNS rebinding and HTTP redirects. Attackers can craft URLs that resolve to internal services after the initial validation check, enabling the headless browser to follow redirects and read internal responses including sensitive canary values. |
| CVE-2026-56003 | A heap buffer overflow due to missing size checking in the property buffer when parsing PCF files in libXfont2 ComputeScaledProperties() before libXfont2 before 2.0.8 could be used by attackers using authenticated X clients to execute code within the X server. |
| CVE-2026-54329 | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, the Accessories API create path mass-assigns request parameters to the Accessory model while company_id is mass assignable, allowing a low-privileged authenticated user in one company to create accessory records under another company when Full Multiple Companies Support is enabled. This issue is fixed in version 8.6.2. |
| CVE-2026-57771 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Milan Petrovic GD Rating System gd-rating-system allows Blind SQL Injection.This issue affects GD Rating System: from n/a through <= 3.7. |
| CVE-2026-50340 | Use after free in Windows Runtime allows an authorized attacker to elevate privileges over a network. |
| CVE-2026-57787 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CreativeWS CWS SVGicons cws-svgicons allows Blind SQL Injection.This issue affects CWS SVGicons: from n/a through <= 1.5.5. |
| CVE-2026-56001 | A heap buffer overflow in BitmapScaleBitmaps in libXfont2 before 2.0.8 due to an overflowing 32bit size could be used by attackers able to access the X Server to execute code within the X server cont |
| CVE-2026-55999 | Local attackers with a X connection able to provide PCX fonts to the X server xorg-server before 21.2.24 and xwayland before 24.1.13 could cause a heap buffer overflow via SetFont due to missing glyph boundary checks. |
| CVE-2026-56690 | Dell PowerFlex Manager, Version prior to 5.1.0.1, contain(s) an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure, Information exposure, and Unauthorized access. |
| CVE-2026-57772 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP Inventory WP Inventory Manager wp-inventory-manager allows Blind SQL Injection.This issue affects WP Inventory Manager: from n/a through <= 2.4.0. |
| CVE-2026-50520 | Improper neutralization of special elements used in a command ('command injection') in Visual Studio Code allows an unauthorized attacker to execute code locally. |
| CVE-2026-54122 | Heap-based buffer overflow in Windows GDI+ allows an unauthorized attacker to execute code locally. |
| CVE-2026-0487 | SAProuter on Microsoft Windows allows an unauthenticated attacker to load library (DLL) files from an untrusted location, allowing them to execute malicious code on the system. This could enable the attacker to hijack the DLL loading process and achieve arbitrary code execution. This has high impact on confidentiality, integrity and availability of the system. |
| CVE-2026-57432 | Perl versions through 5.43.10 have an integer overflow in S_measure_struct leading to an out-of-bounds heap read in pack and unpack. S_measure_struct adds each item's size times its repeat count to a running total with no overflow check, so a large repeat count in a pack or unpack template wraps the signed SSize_t total negative. The @, X, and x position codes then guard their moves with a signed length comparison that passes when the length is negative, advancing the buffer pointer out of bounds. A template derived from untrusted input can read heap memory past the buffer and return it to the caller. |
| CVE-2026-54992 | Heap-based buffer overflow in Windows Message Queuing Queue Manager allows an unauthorized attacker to execute code locally. |
| CVE-2026-49184 | Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. |
| CVE-2026-62195 | OpenClaw versions 2026.5.20 before 2026.6.6 contain an authorization bypass vulnerability in the MCP loopback feature that allows lower-trust callers to execute owner-only tools. Attackers can bypass authorization checks through configured input paths to execute or persist actions beyond their intended permissions. |
| CVE-2026-55427 | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, `coder config-ssh` wrote server-supplied SSH settings (`HostnameSuffix`, `SSHConfigOptions`) into the user's `~/.ssh/config` without sanitizing embedded newlines or restricting directives so a malicious or compromised Coder server could inject arbitrary SSH configuration. Practical exploitation requires control of the server-supplied values through a malicious or compromised deployment, a man-in-the-middle position or admin access to the `HostnameSuffix` and `SSHConfigOptions` settings. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 validates `HostnameSuffix` and `SSHConfigOptions` against a strict character set that rejects newlines and other control characters. As a workaround, inspect `coder config-ssh --dry-run` output before applying changes. |
| CVE-2026-58596 | Untrusted pointer dereference in Microsoft Edge (Chromium-based) allows an unauthorized attacker to elevate privileges over a network. |
| CVE-2026-57850 | RustDesk before 1.4.9 does not enforce a session's authorized connection scope on the server side, so a peer granted a limited session type (FileTransfer, PortForward, ViewCamera, or Terminal) can send control messages and login options reserved for a full Remote session. An authenticated remote peer can exploit this missing scope check to act outside its granted scope, injecting out-of-scope control messages to observe and control the host beyond the permissions it was given. |
| CVE-2026-15122 | Insufficient validation of untrusted input in Codecs in Google Chrome on Windows prior to 150.0.7871.115 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) |

| | |
|---|---|
| CVE-2026-55830 | RestrictedPython is a tool that helps to define a subset of the Python language which allows to provide a program input into a trusted environment. Prior to 8.3, check_function_argument_names() rejected protected guard hook names for regular, variadic, and keyword-only arguments but omitted positional-only arguments, allowing __getattr__, _getitem_, _write_, or _print_ to be shadowed by a local parameter and bypass the embedding application's access policy. This issue is fixed in version 8.3. |
| CVE-2026-56241 | Capgo before 12.128.2 contains a privilege escalation vulnerability where demoted super_admin users retain access to delete_non_compliant_bundles and count_non_compliant_bundles RPCs due to stale org_users.user_right column not being cleared during role binding deletion. Attackers can exploit this by maintaining a previously granted super_admin role to enumerate and bulk delete non-compliant bundles across the entire organization indefinitely. |
| CVE-2026-58281 | Deserialization of untrusted data in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network. |
| CVE-2026-15119 | Race in GetUserMedia in Google Chrome prior to 150.0.7871.115 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-62196 | OpenClaw versions 2026.3.22 before 2026.6.6 contain an authorization bypass vulnerability where WhatsApp group IDs can satisfy elevated sender allowlists. Attackers with lower-trust access can perform actions requiring stronger authorization by leveraging group ID validation in the affected feature. |
| CVE-2026-15120 | Use after free in Core in Google Chrome on Windows prior to 150.0.7871.115 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-56675 | 9Router is an AI router & token saver. Prior to 0.5.2, 9router treats loopback requests as trusted and allows /v1/* access without an API key, so a same-host reverse proxy that forwards public traffic to the backend through 127.0.0.1 causes src/dashboardGuard.js to misclassify external requests as local. A remote unauthenticated attacker can access /v1 APIs such as /v1/models and may abuse configured upstream provider credentials through /v1 proxy endpoints depending on enabled providers. This issue is fixed in version 0.5.2. |
| CVE-2026-56305 | Capgo before 12.128.2 contains an authentication bypass vulnerability in the password change endpoint that allows attackers to change user passwords without requiring current password confirmation. Attackers with temporary session access can exploit this flaw to permanently lock out legitimate users and achieve full account takeover. |
| CVE-2026-15736 | Snowflake SQLAlchemy versions prior to 1.11.0 contain several security vulnerabilities, including: Improper handling of user-supplied column identifiers in merge operations could allow SQL injection through attacker-controlled input keys. An attacker may be able to exploit this through request field names in a dynamic upsert endpoint, potentially enabling read access to data visible to the application's database role or modification of values within the same MERGE statement. Improper literal rendering of bound parameters when building certain Snowflake-specific table creation queries could allow SQL injection. An attacker may be able to exploit this by supplying a crafted string to any application endpoint that passes user-controlled data through the affected query-building API, potentially causing arbitrary data exfiltration within the scope of the connection role. Improper forwarding of connection configuration parameters could allow an attacker to cause the library to read arbitrary local files and transmit their contents to an attacker-controlled endpoint. An attacker may be able to exploit this in deployment environments that accept user-controlled connection parameters, potentially exposing sensitive files accessible to the application process. The fix is available in Snowflake SQLAlchemy version 1.11.0. Users must manually upgrade. |
| CVE-2026-53657 | Lima launches Linux virtual machines, typically on macOS, for running containerd. Prior to 2.1.3, on an instance of Lima running with the qemu driver, an arbitrary user in the VM could access /run/lima-guestagent.sock when the guest agent is enabled, which could result in running arbitrary commands with root privileges in the VM because the guest agent socket provides tunneling for arbitrary addresses, including Unix socket addresses for privileged daemons like D-Bus. This issue is fixed in version 2.1.3. |
| CVE-2026-55428 | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, the tailnet coordinator validates that an agent's `Addresses` derive from its authenticated UUID but applies no equivalent check to `AllowedIPs`. The coordinator forwards agent-supplied `AllowedIPs` verbatim to tunnel peers which install them into the WireGuard peer configuration. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 validates each `AllowedIPs` prefix against the authenticating agent's UUID just like `Addresses`. As a workaround, monitor coordinator logs for agents advertising unexpected `AllowedIPs` prefixes. |
| CVE-2026-59731 | Astro is a web framework for content-driven websites. Version 6.4.7 performs authorization decisions on a partially decoded pathname after reaching the iterative URL decoder limit, while later rewrite route matching performs an additional decodeURI() operation and can resolve the request to a protected route. This issue is fixed in version 6.4.8. |
| CVE-2026-59197 | Pillow is a Python imaging library. Prior to 12.3.0, Pillow's public rank-filter API can trigger a native heap out-of-bounds write when given a very large odd filter size because ImageFilter.RankFilter.filter() calls image.expand(size // 2, size // 2) before rank-filter size validation and ImagingExpand() computes output dimensions with unchecked signed int arithmetic. This issue is fixed in version 12.3.0. |
| CVE-2026-58477 | Sustainable Irrigation Platform (SIP) through version 5.2.16 contains a mass assignment vulnerability that allows unauthenticated attackers to overwrite sensitive configuration settings by supplying arbitrary parameter names in HTTP requests. Attackers can manipulate parameters corresponding to sensitive values such as the passphrase and listening port, and can also achieve the same result through cross-site request forgery due to the absence of adequate request validation. |
| CVE-2026-58525 | Improper access control in Microsoft Edge (Chromium-based) allows an unauthorized attacker to bypass a security feature over a network. |
| CVE-2026-56259 | Crawl4AI before 0.8.8 contains credential exfiltration vulnerabilities in the Docker API server that allow attackers to redirect LLM API calls to attacker-controlled endpoints and read arbitrary environment variables. Attackers can exploit the unauthenticated /md, /llm, and /llm/job endpoints by supplying a malicious base_url parameter and setting api_token to env:VARIABLE_NAME to exfiltrate provider API keys and server secrets including JWT SECRET_KEY for authentication bypass. |
| CVE-2026-57239 | The user-controllable executable files will be directly executed by high-privilege processes, allowing low-privilege users to have the opportunity to elevate their privileges to NT AUTHORITY\SYSTEM. |
| CVE-2026-44787 | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, the signup flow could allow newly registered users to set primary_group_id and gain whisper-group privileges without legitimate group membership on sites with whispers_allowed_groups configured. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5. |
| CVE-2026-29009 | U-Boot through 2026.04-rc3 contains a buffer overflow vulnerability in nfs_readlink_reply() (net/nfs-common.c) when CONFIG_CMD_NFS is enabled, allowing a malicious or compromised NFS server to overflow the 2048-byte nfs_path_buff buffer by returning multiple relative symlink targets that are appended without cumulative length validation. Attackers can send two or more READLINK responses containing relative symlink targets of approximately 1100 bytes each to corrupt adjacent BSS variables including nfs_server_ip, nfs_server_mount_port, nfs_server_port, nfs_our_port, nfs_state, and rpc_id, potentially achieving memory corruption and control over the NFS client state machine. |

| | |
|---|---|
| CVE-2026-29519 | Lucee CFML Server versions across the 5.3.x, 6.1.x, 6.2.x, and 7.0.x release lines contain a reflected cross-site scripting vulnerability in URL path parsing that allows unauthenticated remote attackers to execute arbitrary JavaScript in a victim's browser by embedding HTML or JavaScript payloads within the request path. Attackers can craft a malicious URL containing injected script content that is reflected in the server's response without proper output encoding, enabling session hijacking or unauthorized actions against the Lucee administrative interface when a victim visits the crafted link. |
| CVE-2026-4256 | Improper neutralization of special elements used in an LDAP query ('LDAP injection') vulnerability in PEAKUP Technology Inc. PassGate allows LDAP Injection. This issue affects PassGate: through 30042026. |
| CVE-2026-50429 | Out-of-bounds read in Windows Kernel allows an unauthorized attacker to disclose information over a network. |
| CVE-2026-48363 | ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Uncontrolled Search Path Element vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed. |
| CVE-2026-10672 | subsys/net/lib/lwm2m/lwm2m_pull_context.c copied the firmware-update Package URI into a fixed static buffer (context.uri, size CONFIG_LWM2M_SWMGMT_PACKAGE_URI_LEN, default 128) with memcpy(context.uri, uri, LWM2M_PACKAGE_URI_LEN), copying exactly the destination size with no length validation. The Firmware-Update object stores the server-supplied Package URI (/5/0/1) in a 255-byte buffer, so a LwM2M management server (or an on-path attacker on a session lacking strong DTLS) can WRITE a URI of 128-254 characters; only the first 128 bytes are then copied into context.uri with no NUL terminator. That buffer is subsequently consumed as a C string by http_parser_parse_url(context.uri, strlen(context.uri), ...), strlen-based CoAP URI-path/PROXY-URI option appends, and lwm2m_parse_peerinfo(), causing an out-of-bounds read of adjacent static memory. The over-read bytes are appended to outbound CoAP requests (information disclosure of adjacent device memory to the server/proxy) and can crash the device (denial of service). The vulnerable copy was introduced by the pull-context refactor (first released in v3.0.0) and is present through v4.4.0; the default-on CONFIG_LWM2M_FIRMWARE_UPDATE_PULL_SUPPORT path is affected. The fix adds a strlen(uri) >= sizeof(context.uri) check returning -ENOMEM and switches to strcpy(), guaranteeing a bounded, NUL-terminated buffer. |
| CVE-2026-59802 | PasswordPusher before 2.8.1 accepts data URI schemes in URL push payloads due to insufficient validation in the valid_url function. Attackers can create malicious pushes containing data:text/html URIs that execute arbitrary JavaScript in victims' browsers when clicked, enabling phishing and credential theft under the trusted PasswordPusher domain. |
| CVE-2026-48364 | ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Uncontrolled Search Path Element vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed. |
| CVE-2026-59822 | LiteLLM is a proxy server (AI Gateway) to call LLM APIs in OpenAI (or native) format. Prior to 1.84.0, LiteLLM's MCP Streamable HTTP endpoint allowed an unauthenticated attacker to use a fabricated Authorization header to trigger an OAuth2 passthrough fallback path that replaced failed LiteLLM key validation with an empty UserAPIKeyAuth() object, allowing requests to reach MCP tooling without a valid LiteLLM key. This issue is fixed in version 1.84.0. |
| CVE-2026-50338 | Improper authentication in Azure Spring Apps allows an authorized attacker to elevate privileges over a network. |
| CVE-2026-44752 | SAP NetWeaver Application Server Java allows an unauthenticated attacker to inject malicious JavaScript through crafted URLs. When a victim accesses such a URL, the script executes in the user's browser, allowing the attacker to access sensitive session information and modify non-sensitive data displayed in the client&#65533;s browser. This results in a high impact on confidentiality, low impact on integrity with no impact on availability of the application. |
| CVE-2026-58500 | MCP Appium is an MCP server that provides AI assistants with tools to automate mobile app testing on Android and iOS. In versions prior to 1.85.10, the createLocatorGeneratorUI function interpolates attacker-controlled element attributes — text, content-desc, resource-id, and locator selector values — directly into an HTML template literal without any HTML or JavaScript context escaping. An attacker who controls the UI of the app under test can inject arbitrary HTML and JavaScript into the MCP UI resource returned by the generate_locators tool. When a victim's MCP client renders this resource, the injected script executes and can invoke arbitrary MCP tools via window.parent.postMessage, leading to unauthorized MCP tool execution such as taking screenshots, reading page source, or any other registered capability. This issue has been fixed in version 1.85.10. |
| CVE-2026-55641 | 9Router is an AI router & token saver. Prior to 0.5.2, 9router determines whether a /v1 LLM proxy request is local by reading the client-controlled Host header, allowing a remote unauthenticated attacker to send Host: localhost and bypass API-key authentication. In the default configuration, this exposes the /v1 proxy to upstream provider calls using stored provider credentials and allows /v1/search with the searxng provider_options.baseUrl parameter to drive server-side requests to internal or cloud-metadata hosts. This issue is fixed in version 0.5.2. |
| CVE-2026-54423 | In OpenStack Ironic before 37.0.1, an Ironic user with the ability to deploy nodes using the IPMI management interface can maliciously use the send_raw step to send arbitrary IPMI commands to a node, bypassing Ironic's access control. |
| CVE-2026-58499 | EverOS is a memory runtime for agents. Prior to 1.0.1, EverOS is vulnerable to path traversal in the POST /api/v1/memory/add ingestion endpoint because the per-message sender_id field was not validated as a path-safe identifier, unlike app_id and project_id. During user-memory extraction, sender_id is used as owner_id and joined into the filesystem path where the extracted episode is persisted as a Markdown file, so a sender_id containing ../ sequences could direct writes outside the configured memory root and allow an unauthenticated caller to create or overwrite .md files at locations writable by the server process with partially attacker-influenced content. This issue is fixed in version 1.0.1. |
| CVE-2026-57768 | Incorrect Privilege Assignment vulnerability in favethemes Houzez Login Register houzez-login-register allows Privilege Escalation.This issue affects Houzez Login Register: from n/a through <= 3.3.3. |
| CVE-2026-33390 | An Incorrect Privilege Assignment vulnerability was discovered in the synchronization functionality due to Arc sensors receiving CLI permissions. An authenticated user with limited privileges can push administrative CLI commands through the sync, altering the device configuration, and/or affecting its availability. |
| CVE-2026-55809 | Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Flag attendance field allows Object Injection. This issue affects Flag attendance field versions: from 0.0.0 to 1.2. |
| CVE-2026-56169 | Improper authentication in Windows Admin Center allows an authorized attacker to elevate privileges over a network. |
| CVE-2026- | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in stmcan RT-Theme 18 \| Extensions rt18- |

| | |
|---|---|
| 57743 | extensions allows PHP Local File Inclusion.This issue affects RT-Theme 18 \| Extensions: from n/a through <= 2.5. |
| CVE-2026-55810 | Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Plotly.js Graphing allows Object Injection. This issue affects Plotly.js Graphing versions: from 0.0.0 to 3.0.2. |
| CVE-2026-35552 | In CAXperts UPVWebServices 2.4.2212.603 through 2.7.6 and UDiTH Portal 2026.0.0 through 2026.2.0, an authenticated remote user can invoke an administrative API endpoint intended for privileged users. Due to missing authorization checks, this allows the attacker to deactivate the application's license. |
| CVE-2026-58595 | Improper restriction of rendered ui layers or frames in Microsoft Bing App for IOS allows an unauthorized attacker to perform spoofing over a network. |
| CVE-2026-54591 | AsyncSSH is a Python package which provides an asynchronous client and server implementation of the SSHv2 protocol on top of the Python asyncio framework. Prior to 2.23.1, a malicious SSH server can write arbitrary files on the asyncssh SCP client's filesystem by sending filenames containing ../ traversal sequences because _parse_cd_args in scp.py returns server-provided names verbatim and _recv_files joins them to the destination path without enforcing the target directory boundary. This issue is fixed in version 2.23.1. |
| CVE-2026-54995 | Use after free in Reliable Multicast Transport Driver (RMCAST) allows an unauthorized attacker to execute code over a network. |
| CVE-2026-31985 | When the upstream Guardian or CMC was configured in the Remote Collector via n2os-tui, the generated configuration disabled TLS certificate verification, and no option was provided to enable it. A malicious actor could perform a man-in-the-middle attack and intercept the communication between the Remote Collector and the Guardian or CMC. This could result in theft of the sync token, impersonation of the server, injection of spoofed data (such as false asset information or vulnerabilities) into the Guardian or CMC, or disruption of the data flow between the Remote Collector and the Guardian or CMC. |
| CVE-2026-7655 | The SureCart plugin for WordPress is vulnerable to privilege escalation via account takeover in versions up to, and including, 4.2.3. This is due to the plugin not properly validating a user's identity prior to updating their details like email during customer profile synchronization from webhook events. This makes it possible for unauthenticated attackers to change linked user's email addresses, including administrators if the administrator account is linked to a SureCart customer record, and leverage that to reset the user's password and gain access to their account if the customer ID is known. |
| CVE-2026-58065 | The Apache Airflow Git provider runs its git-over-SSH operations with `StrictHostKeyChecking=no` by default, disabling SSH host-key verification. An attacker who can intercept the network path between an Airflow worker and the Git server can impersonate the server (man-in-the-middle), capturing the SSH deploy key or injecting malicious repository content. Deployments that use the Git DAG bundle or Git provider to clone over SSH with a deploy key are affected. The fix changes the default to verify host keys; upgrade to apache-airflow-providers-git `0.4.1` or later and configure a `known_hosts` file. |
| CVE-2026-58476 | Sustainable Irrigation Platform (SIP) through version 5.2.16 contains a cross-site request forgery vulnerability that allows remote attackers to perform state-changing administrative actions by luring a logged-in administrator into visiting a malicious page that issues HTTP GET requests without CSRF token validation or origin verification. Attackers can trigger actions such as disabling the passphrase, rebooting the device, deleting programs, or installing plugins, with the default configuration exposing these endpoints to unauthenticated users due to no required passphrase and a default credential of 'opendoor'. |
| CVE-2026-44745 | SAP Approuter does not properly validate incoming request headers during the OAuth2 login flow under certain configurations. This allows an unauthenticated remote attacker to craft a malicious link which, when clicked by a victim, could lead to unauthorized access. Successful exploitation results in a high impact to the confidentiality and integrity with no impact on the availability of the application. |
| CVE-2026-56668 | ZITADEL is an open source identity management platform. Prior to 4.15.3, ZITADEL's OAuth2 Token Exchange endpoint for urn:ietf:params:oauth:grant-type:token-exchange does not verify that the subject token belongs to the requesting client or that requested scopes remain within the original token's scopes, allowing a low-privilege token to be exchanged for elevated permissions at another application. This issue is fixed in version 4.15.3. |
| CVE-2026-51923 | An Insecure Direct Object Reference (IDOR) vulnerability exists in docuForm GmbH Client v.11.11c allowing a remote attacker to execute arbitrary code via the user settings component, and modify or retrieve sensitive data associated with other users’ accounts. |
| CVE-2026-51925 | A Local File Inclusion (LFI) vulnerability exists in docuForm GmbH Client v.11.11c that allows a remote attacker to execute arbitrary code via the dfm-menu_report.php component. Attackers can exploit this flaw to read arbitrary files on the server, including sensitive configuration files, source code or system files. |
| CVE-2026-3144 | IBM API Connect 12.1.0.0 through 12.1.0.3 uses default credentials which could allow an attacker to gain unauthorized access to the application before the system enforces a credential update. |
| CVE-2026-42900 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows App Store allows an unauthorized attacker to elevate privileges over a network. |
| CVE-2026-3688 | The WCFM Membership – WooCommerce Memberships for Multivendor Marketplace plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.11.10. This is due to the 'wcfmvm_membership_change' AJAX action not validating user permission to modify other users. This makes it possible for authenticated attackers, with vendor level access and above, to change any user's role to 'wcfm_vendor' by changing their membership plan. |
| CVE-2026-12598 | The LoginPress Pro plugin for WordPress is vulnerable to authentication bypass in versions up to and including 6.2.3 via the Spotify Social Login addon. This is due to the loginpress_on_spotify_login() function trusting the unverified 'email' field returned by Spotify's /v1/me endpoint and using it directly with get_user_by('email', $profile['email']) to identify and log in an existing WordPress account, without confirming that the Spotify user actually owns the email address (Spotify documents that the profile email is unverified) and without requiring the user to prove ownership of the matching WordPress account. This makes it possible for unauthenticated attackers to log in as any existing WordPress user, including Administrators, by registering a Spotify account using the targeted user's email address and authenticating via the Spotify provider. |
| CVE-2026-49164 | Heap-based buffer overflow in Active Directory Domain Services allows an unauthorized attacker to execute code over a network. |
| CVE-2026-55377 | Logto is the modern, open-source auth infrastructure for SaaS and AI apps. Prior to 1.41.0, Logto's Account Center step-up check accepted any active verification record that belonged to the current user and had isVerified === true. A WebAuthn registration verification record for binding a new passkey could be created and verified with only an existing Account API bearer token, then sent in the logto-verification-id header and treated as identityVerified=true by Account Center routes, allowing MFA factor management without proving possession of an existing password, identifier, or MFA factor. This issue is fixed in version 1.41.0. |
| CVE- | Frigate is an open source network video recorder. In version 0.17.1, the GET /api/logs/{service} endpoint allows any authenticated user including the viewer role |

| | |
|---|---|
| 2026-54652 | to download Frigate and nginx logs, exposing auto-generated admin passwords and camera credentials logged in request query strings and enabling viewer-to-admin privilege escalation. A fixed release has not been identified. |
| CVE-2026-62192 | OpenClaw versions 2026.6.6 before 2026.6.9 contain an authorization bypass vulnerability in Discord guild actions that allows lower-trust callers to perform actions requiring stronger authorization checks. Attackers can exploit misconfigured input paths to skip cross-provider requester authorization and execute restricted operations. |
| CVE-2026-12597 | The LoginPress Pro plugin for WordPress is vulnerable to Authentication Bypass via the GitHub OAuth callback in versions up to, and including, 6.2.3. The vulnerability exists in the loginpress_on_github_login() function, which blindly trusts the first element (profile[0]['email']) of the array returned by GitHub's /user/emails endpoint as an account-binding identifier without verifying that the email carries a verified === true status. This makes it possible for unauthenticated attackers to log in as any existing WordPress user, including administrators, by adding an unverified email address matching a local account to their GitHub profile and triggering the OAuth callback via a crafted code parameter — causing the plugin to call get_user_by('email', ...) and establish an authenticated session for the matched account. Practical exploitation is conditional on GitHub returning the attacker-added unverified email at index 0 of the /user/emails response, as GitHub typically prioritizes the primary verified address first; nonetheless, the absence of any email verification check in the plugin constitutes a fundamental authentication bypass flaw. |
| CVE-2026-62187 | OpenClaw Feishu tools (npm package @openclaw/feishu) in versions <= 2026.6.6 could ignore per-account disablement. A lower-trust caller or a configured input path could perform actions that should have required a stronger authorization or policy check, resulting in unauthorized operations. The issue is fixed in version 2026.6.9. Impact depends on the operator's configuration and whether lower-trust input can reach the affected feature. |
| CVE-2026-62188 | OpenClaw @openclaw/feishu versions 2026.6.6 and earlier contain an incorrect authorization vulnerability in which the Feishu permission tools could ignore per-account disablement settings. When the affected feature is enabled and reachable, a lower-trust caller or configured input path could perform actions that should have required a stronger authorization or policy check. The issue is fixed in version 2026.6.9. |
| CVE-2026-12595 | The LoginPress Pro plugin for WordPress is vulnerable to Authentication Bypass via Unverified OAuth Email in all versions up to and including 6.2.3. The vulnerability exists in the loginpress_on_discord_login() Discord OAuth callback handler, which accepts the email field returned by Discord's /users/@me endpoint without ever checking that the profile's verified flag is true, then directly maps that email to a local WordPress account via get_user_by('email', $profile['email']) and issues an authenticated session cookie via wp_set_auth_cookie(). This makes it possible for unauthenticated attackers to take over any existing WordPress account — including administrator accounts — by registering a Discord account configured with an unverified email address that matches the target user's registered WordPress email and completing the standard Discord OAuth flow. |
| CVE-2026-56246 | Capgo before 12.128.2 contains a broken access control vulnerability in the organization management API where a scoped API key (limited_to_orgs) inherits its owner-user's permissions, allowing destructive cross-organization actions. When a user is an admin in two organizations and creates a write-mode API key restricted to one organization, that key can still perform destructive operations (e.g., DELETE /organization, DELETE /organization/members) against another organization. The root cause is route-level authorization (rbac_check_permission_direct) that evaluates the key owner's user privileges before enforcing the API key's limited_to_orgs scope. |
| CVE-2026-13244 | Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Tealium iQ Tag Management allows Object Injection. This issue affects Tealium iQ Tag Management versions: from 0.0.0 to 2.4.0. |
| CVE-2026-51924 | An issue in docuForm GmbH Client v.11.11c allows a remote attacker to execute arbitrary code via the file upload and report.php component |
| CVE-2025-45422 | Incorrect access control in Proximus b-box v8c.725A allows authenticated attackers to bypass normal restrictions and make arbitrary changes to port forwarding rules. |
| CVE-2026-50694 | Use after free in Windows Secure Socket Tunneling Protocol (SSTP) allows an unauthorized attacker to execute code over a network. |
| CVE-2026-11963 | The User Registration & Membership WordPress plugin before 5.2.2 does not perform an authorization check on a membership-upgrade action and derives the user to modify from a caller-supplied identifier instead of the current user, allowing any authenticated user such as a subscriber to change another user's WordPress role and membership tier. |
| CVE-2026-59245 | In the Apache Airflow FAB auth manager, a DAG whose `dag_id` is `DAGs` collided with the global all-DAGs permission resource name produced by `resource_name()`, so a user granted per-DAG `access_control` on that one DAG was silently granted the global all-DAGs permission (privilege escalation). The escalation triggers when a DAG named `DAGs` exists and a lower-privileged user is given per-DAG access to it, granting that user read/edit access to every DAG. Users are advised to upgrade to `apache-airflow-providers-fab` 3.7.2 or later, which disambiguates the resource-name collision. |
| CVE-2026-59796 | In JetBrains TeamCity before 2026.1.2 pipeline modification was possible due to improper permission checks |
| CVE-2026-59795 | In JetBrains TeamCity before 2026.1.2 stored XSS via unauthenticated agent registration was possible |
| CVE-2026-54771 | Langroid is a framework for building large-language-model-powered applications. Prior to version 0.65.3, a Langroid application exposing a chat interface to untrusted users may allow direct tool invocation via raw JSON payloads, even when tools are registered with `use=False, handle=True`. Version 0.65.3 fixes the issue. |
| CVE-2026-49213 | TypeBot is a chatbot builder tool. Prior to 3.17.2, Typebot's shared SSRF validator in packages/lib/src/ssrf/validateHttpReqUrl.ts can be bypassed with the IPv6 unspecified address :: because validateIPAddress blocks local, metadata, and private ranges but does not block :: or its expanded form. A workspace editor or creator can configure a server-side HTTP Request block or guarded script fetch to make the Typebot server connect to local HTTP services through safeKy, including flows triggered by POST /v1/typebots/{publicId}/startChat or POST /v1/sessions/{sessionId}/continueChat. This issue is fixed in version 3.17.2. |
| CVE-2026-12511 | The AI Engine WordPress plugin before 3.5.5 does not sanitize a user-supplied filename before using it to write a downloaded file, allowing authenticated users with editor-level access to write attacker-controlled bytes to an arbitrary location on the server via path traversal. |
| CVE-2026-38057 | The iDirect iQ200 does not validate CSRF tokens on state-changing API endpoints after authentication. The /api/reboot endpoint accepts POST requests authenticated solely by a session cookie that lacks the SameSite attribute. A remote attacker can host a malicious web page that, when visited by an authenticated administrator, automatically submits a cross-site POST request causing an immediate device reboot and satellite link loss. Repeated attacks can sustain a denial-of-service condition. |

| | |
|---|---|
| CVE-2026-50439 | Use after free in Microsoft Message Queuing Queue Manager allows an unauthorized attacker to execute code over a network. |
| CVE-2026-22659 | FlaskBB through 2.2.0, fixed in commit acc88cf, contains an authorization bypass vulnerability that allows authenticated moderators to perform unauthorized actions on topics in forums they do not control by submitting crafted topic ID lists. Attackers can include a low-ID topic from a permitted forum as an anchor in a batch request, causing the permission check applied only to the first result to pass, and then execute lock, unlock, delete, or hide actions against topics in unmoderated forums. |
| CVE-2026-10666 | parse_ipv4() in subsys/net/ip/utils.c (reached via net_ipaddr_parse() for strings of the form "a.b.c.d:port") copies the port substring into a fixed 17-byte stack buffer (char ipaddr[NET_IPV4_ADDR_LEN + 1]) using a length of str_len - end - 1, where str_len is the full, unbounded input length and end is only the (<=15-byte) offset of the ':' delimiter. Because the destination size is never consulted, a crafted address string with a long suffix after the colon (e.g. "1.2.3.4:" followed by hundreds of bytes) causes an out-of-bounds stack write whose length and contents are fully attacker-controlled (memcpy of the suffix plus a trailing NUL), enabling memory corruption and at minimum a denial of service, and potentially control-flow hijack. The parser is reached from the standard socket API (zsock_getaddrinfo / literal-address resolution), DNS server-string configuration, and the eswifi Wi-Fi co-processor DNS-response path, so an application that resolves a network-influenced address string is exposed. The bug was introduced when the parser was added (Zephyr v1.9.0) and shipped in all releases through v4.4.0. The fix removes the unbounded copy and validates the port length before copying into a small dedicated buffer. Note: the equivalent IPv6 "[addr]:port" path in parse_ipv6() retains the same unbounded copy at this commit and remains a separate, still-reachable instance of the defect. |
| CVE-2026-12378 | The Appointment Booking Calendar Plugin and Scheduling Plugin WordPress plugin through 1.1.28 does not validate data before passing it to a PHP deserialization function, allowing unauthenticated attackers to inject arbitrary PHP objects; where a suitable gadget chain is present on the site this can be leveraged to achieve remote code execution. |
| CVE-2026-56313 | Capgo before 12.128.2 contains a cross-organization account disruption vulnerability in the SSO prelink endpoint that allows enterprise administrators to delete password identities of users in foreign organizations. Attackers with org.update_settings permission and an active SSO provider can call the prelink-users endpoint to permanently remove email-based authentication for any user matching the provider's email domain, forcing victims to use the attacker's SSO provider or complete password reset recovery. |
| CVE-2026-12583 | The Newsletters WordPress plugin before 4.15 does not prevent deserialization of untrusted input that is stored through a public form, allowing unauthenticated attackers to inject a PHP object and, via a property-oriented gadget chain bundled with the Newsletters WordPress plugin before 4.15, write arbitrary files and execute code on the server. |
| CVE-2026-59224 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.10.0, backend/open_webui/routers/terminals.py built the ws_terminal upstream URL from an unencoded session_id and appended user_id as a query parameter, allowing query injection to make the terminal backend resolve another user identity; the HTTP proxy path also forwarded X-User-Id as an integrity-unbound identity claim. This issue is fixed in version 0.10.0. |
| CVE-2026-42975 | Heap-based buffer overflow in Windows Bluetooth Port Driver allows an unauthorized attacker to execute code over an adjacent network. |
| CVE-2026-15293 | The WP Business Intelligence Lite plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.2.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify stored SQL queries, which can lead to privilege escalation via arbitrary SQL execution when the modified query is viewed by an administrator. |
| CVE-2026-40400 | Relative path traversal in Windows PowerShell allows an authorized attacker to execute code over a network. |
| CVE-2026-50365 | Improper authentication in Windows RPC API allows an unauthorized attacker to elevate privileges over an adjacent network. |
| CVE-2026-58647 | Improper neutralization of input during web page generation ('cross-site scripting') in Power BI allows an authorized attacker to perform spoofing over a network. |
| CVE-2026-49169 | Use after free in DNS Server allows an authorized attacker to execute code over a network. |
| CVE-2026-11903 | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Progress MOVEit Transfer (Ad Hoc module). This issue affects MOVEit Transfer: from 2026.0.0 before 2026.0.1, from 2025.1.0 before 2025.1.4, from 2025.0.0 before 2025.0.8. |
| CVE-2026-49176 | Improper privilege management in Windows WalletService allows an authorized attacker to elevate privileges locally. |
| CVE-2026-58610 | Heap-based buffer overflow in Microsoft Windows Media Foundation allows an unauthorized attacker to execute code locally. |
| CVE-2026-58635 | Improper neutralization of special elements used in a command ('command injection') in Windows Narrator Braille allows an authorized attacker to elevate privileges locally. |
| CVE-2026-34196 | Software installed and run as a non-privileged user may conduct improper GPU system calls to cause an integer overflow and map two GPU virtual addresses to the same physical address. One of these virutal mappings can be freed along with the physical page, allowing for a read/write UAF via the second mapping The second virtual mapping references a physical address that has been freed after the first virtual mapping has been freed. This allows the physical memory to be allocated (for example) by another process and read/written to. |
| CVE-2026-58618 | Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally. |
| CVE-2026- | Improper authorization in Windows Admin Center allows an authorized attacker to execute code locally. |

| | |
|---|---|
| 58631 | |
| CVE-2026-44800 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally. |
| CVE-2026-49175 | Heap-based buffer overflow in Windows DNS allows an authorized attacker to elevate privileges locally. |
| CVE-2026-58636 | Improper link resolution before file access ('link following') in Window PC Manager allows an authorized attacker to elevate privileges locally. |
| CVE-2026-49173 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally. |
| CVE-2026-49170 | Insufficient granularity of access control in Windows StateRepository API allows an authorized attacker to elevate privileges locally. |
| CVE-2026-49166 | Use after free in Microsoft Printer Drivers allows an authorized attacker to elevate privileges locally. |
| CVE-2026-48581 | Insufficient granularity of access control in Microsoft Surface allows an authorized attacker to elevate privileges locally. |
| CVE-2026-47296 | Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges locally. |
| CVE-2026-58609 | Out-of-bounds read in Microsoft Graphics Component allows an unauthorized attacker to execute code locally. |
| CVE-2026-42982 | Improper validation of consistency within input in Windows Secure Kernel Mode allows an authorized attacker to elevate privileges locally. |
| CVE-2026-10669 | On Xtensa SoCs built with CONFIG_XTENSA_MPU and CONFIG_USERSPACE, arch_buffer_validate() in arch/xtensa/core/mpu.c — the architecture hook that verifies a user-mode-supplied buffer is accessible to the calling user thread with the requested permission — defaulted its return value to 0 (access permitted) and only set a denial result inside its per-MPU-region probe loop. When the rounded extent of the buffer wraps the 32-bit address space (size + alignment offset near SIZE_MAX, or ROUND_UP(size + offset) overflowing to 0), the loop executes zero iterations and the function returns 0 = permitted without probing any MPU region. The syscall-layer pre-checks (K_SYSCALL_MEMORY_SIZE_CHECK / Z_DETECT_POINTER_OVERFLOW) only catch a raw addr+size wrap and do not cover the ROUND_UP-induced wrap, and the string path (arch_user_string_nlen -> arch_buffer_validate) has no syscall-layer guard at all. An unprivileged user-mode thread can therefore pass a crafted (addr, size) to any syscall that validates user buffers via k_usermode_from_copy/to_copy or k_usermode_string_copy and have validation succeed for memory it must not access; the kernel then reads from (disclosure) or, with write=1, writes to (corruption) attacker-chosen kernel or other-partition memory on the thread's behalf, enabling information disclosure, memory corruption, privilege escalation, and denial of service. Affected from v3.7.0 (when Xtensa MPU userspace support was added) through v4.4.0. The fix changes the default to -EINVAL (deny by default), adds an explicit size_add_overflow check, and sets the success value only after the full range has been validated. |
| CVE-2026-61437 | PraisonAI (pip package praisonaiagents) before 1.6.78 contains an unsafe dynamic module loading vulnerability in AgentFlow._resolve_pydantic_class (src/praisonai-agents/praisonaiagents/workflows/workflows.py). When a workflow step uses a string output_pydantic reference, the framework locates and imports a sibling tools.py from the workflow file's directory via importlib exec_module without sandboxing, ignoring the PRAISONAI_ALLOW_*_TOOLS environment variables. An attacker who controls a workflow file and its sibling tools.py can execute arbitrary Python code with the workflow runner's privileges when the workflow is executed via WorkflowManager or after load_yaml. |
| CVE-2026-47829 | Argument Injection in bosh-cli allows a compromised BOSH Director to inject arbitrary OpenSSH options into the locally-spawned ssh process when an operator runs bosh ssh -c, bosh logs -f, or other non-interactive SSH paths, leading to local command execution on the operator's workstation. Affected versions: bosh-cli versions prior to v7.10.4. |
| CVE-2026-59858 | Vim is an open source, command line text editor. Prior to 9.2.0735, the C omni-completion script in runtime/autoload/ccomplete.vim interpolates the typeref: or typename: extension field of a tags entry, without escaping, into a :vimgrep pattern that is run through :execute. Because :vimgrep honors the bar as a command separator, a crafted tag field can close the search pattern and append an arbitrary Ex command; opening a hostile .c file whose project tags file contains such an entry and invoking C omni-completion runs that command as the editing user. This issue is fixed in version 9.2.0735. |
| CVE-2026-41154 | Software installed and run as a non-privileged user may cause OOB kernel memory reads or writes through GPU API calls. When indexing pages larger than 4kB in the page freeing logic of the sparse memory implementation, incorrect buffer indexing leads to OOB access. |
| CVE-2026-50351 | Improper access control in Windows Audio Compression Manager (ACM) allows an authorized attacker to elevate privileges locally. |
| CVE-2026-55006 | Insufficient granularity of access control in Microsoft Exchange Server allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50308 | Integer underflow (wrap or wraparound) in Windows NTFS allows an unauthorized attacker to execute code locally. |
| CVE-2026- | Improper access control in Windows Server allows an authorized attacker to elevate privileges locally. |

| | |
|---|---|
| 50311 | |
| CVE-2026-55004 | Double free in Microsoft Printer Drivers allows an authorized attacker to elevate privileges locally. |
| CVE-2026-55002 | External control of file name or path in SQL Server allows an authorized attacker to elevate privileges locally. |
| CVE-2026-55001 | Improper certificate validation in Windows Active Directory allows an authorized attacker to elevate privileges locally. |
| CVE-2026-47290 | Use after free in Microsoft Office allows an unauthorized attacker to execute code locally. |
| CVE-2026-50333 | Missing authentication for critical function in Windows Spaceport.sys allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50675 | Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally. |
| CVE-2026-55011 | Integer underflow (wrap or wraparound) in Microsoft Defender allows an unauthorized attacker to execute code locally. |
| CVE-2026-54993 | Heap-based buffer overflow in Microsoft Windows Media Foundation allows an unauthorized attacker to execute code locally. |
| CVE-2026-54991 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges locally. |
| CVE-2026-54987 | Heap-based buffer overflow in Windows Overlay Filter allows an authorized attacker to elevate privileges locally. |
| CVE-2026-54986 | Heap-based buffer overflow in Windows Win32K allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50697 | Exposure of sensitive information to an unauthorized actor in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally. |
| CVE-2026-58459 | gpsd through release-3.27.5, fixed at commit 4c06658, contains a command injection vulnerability in gpsprof that allows attackers who control the GPS device subtype value to execute arbitrary shell commands by embedding backtick payloads in the gnuplot plot title without proper escaping. The subtype field sourced from a DEVICES JSON log entry or NMEA PGRMT sentence is written into a generated gnuplot program via a set title statement with only double-quote characters escaped, enabling arbitrary shell command execution as the user running gnuplot when the victim renders the generated plot through the gpsprof and gnuplot workflow. |
| CVE-2026-54109 | Integer overflow or wraparound in Windows Resilient File System (ReFS) allows an authorized attacker to execute code locally. |
| CVE-2026-54112 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K allows an authorized attacker to elevate privileges locally. |
| CVE-2026-55009 | Deserialization of untrusted data in Microsoft Exchange Server allows an authorized attacker to elevate privileges locally. |
| CVE-2026-55012 | Integer overflow or wraparound in Microsoft Defender allows an unauthorized attacker to execute code locally. |
| CVE-2026-58602 | Use after free in Windows Kernel Mode Driver allows an authorized attacker to elevate privileges locally. |
| CVE-2026-49796 | Heap-based buffer overflow in Windows GDI+ allows an unauthorized attacker to execute code locally. |
| CVE-2026-58601 | Heap-based buffer overflow in Virtual Hard Disk (VHD) Miniport Driver allows an authorized attacker to elevate privileges locally. |
| CVE-2026-45196 | Kernel software installed and running inside a Host VM may post improper commands to the GPU Firmware to trigger a GPU register access which can lead to privilege escalation. |
| | |

| | |
|---|---|
| CVE-2026-45203 | Kernel software installed and running inside a Host VM may post improper commands to the GPU Firmware to trigger a memory write outside the permitted range of memory for the host kernel. A TOCTOU bug existed where a malicious driver could modify values in memory after firmware validation but before use. |
| CVE-2026-49783 | Improperly implemented security check for standard in Windows Secure Boot allows an authorized attacker to bypass a security feature locally. |
| CVE-2026-54114 | Use after free in Windows Win32K allows an authorized attacker to elevate privileges locally. |
| CVE-2026-59856 | Vim is an open source, command line text editor. Prior to 9.2.0736, the PHP omni-completion script in runtime/autoload/phpcomplete.vim interpolates a class or trait name, taken from the contents of the edited buffer, into a search() pattern that is run via win_execute() without escaping. A name containing a single quote can terminate the search() string argument early, and because the bar is honored as an Ex command separator, the remainder of the name is run as Ex commands; via the :! command this allows arbitrary operating-system command execution when a victim opens a crafted PHP file and invokes omni-completion. This issue is fixed in version 9.2.0736. |
| CVE-2026-49792 | Numeric truncation error in Windows Resilient File System (ReFS) allows an authorized attacker to execute code locally. |
| CVE-2026-49793 | Heap-based buffer overflow in Windows Resilient File System (ReFS) allows an authorized attacker to execute code locally. |
| CVE-2026-49797 | Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. |
| CVE-2026-55014 | Improper access control in Windows Remote Help Defense allows an authorized attacker to elevate privileges locally. |
| CVE-2026-57107 | Improper authentication in Windows Admin Center allows an authorized attacker to elevate privileges locally. |
| CVE-2026-49800 | Integer overflow or wraparound in Windows Web Proxy Auto-Discovery Protocol (WPAD) allows an authorized attacker to elevate privileges locally. |
| CVE-2026-56155 | Insufficient granularity of access control in Active Directory Federation Services (AD FS) allows an authorized attacker to elevate privileges locally. |
| CVE-2026-55948 | Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally. |
| CVE-2026-49808 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Kernel allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50293 | Use after free in Windows Internal Task Bar allows an authorized attacker to elevate privileges locally. |
| CVE-2026-7639 | Software installed and run as a non-privileged user may conduct a sequence of improper GPU system calls causing use after free, which helps in facilitating unprivileged memory access from a shader code. Triggering failure path in the MMU mapping logic by a malicious code could lead to incomplete cleanup of an internal driver state, allowing for future unauthorized access to the contents of the physical memory. |
| CVE-2026-55899 | Stack-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally. |
| CVE-2026-50318 | Stack-based buffer overflow in Windows Resilient File System (ReFS) allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50457 | Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally. |
| CVE-2026-57246 | When dealing with abnormally constructed objects, there is a lack of argument validation; JavaScript triggers signature verification, but the signature plugin does not perform validation when copying the abnormal string, causing the application to crash. |
| CVE-2026-50425 | Use after free in Windows Internal System User Profile allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50335 | Improper access control in Windows Operating Systems allows an authorized attacker to elevate privileges locally. |
| CVE-2026- | Use after free in Content Delivery Manager allows an authorized attacker to elevate privileges locally. |

| | |
|---|---|
| 50427 | |
| CVE-2026-13127 | The application opens the PDF file. JavaScript then rewrites the document to modify the page structure, resulting in the invalidation of the page objects. However, the thumbnails still use the invalid page objects, ultimately causing the application to crash. |
| CVE-2026-57245 | When the application opens a PDF, traverses and builds the annotation elements related to hyperlinks, it fails to validate the abnormal annotation relationships and field combinations. This results in the internal objects entering an invalid state. Eventually, during the destruction phase, an invalid pointer write occurred, causing the application to crash. |
| CVE-2026-50332 | Heap-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50357 | Numeric truncation error in Windows Resilient File System (ReFS) allows an authorized attacker to execute code locally. |
| CVE-2026-50331 | Use after free in Windows Application Model allows an authorized attacker to elevate privileges locally. |
| CVE-2026-13126 | The embedded JavaScript in the PDF deleted the pages, making the object invalid. The application attempted to perform a write operation on the invalid pop-up annotations, resulting in the program crashing. |
| CVE-2026-50433 | Use after free in Windows Media allows an authorized attacker to elevate privileges locally. |
| CVE-2026-39822 | On Unix systems, opening a file in an os.Root improperly follows symlinks to locations outside of the Root when the final path component of the a path is a symbolic link and the path ends in /. For example, 'root.Open("symlink/")' will open "symlink" even when "symlink" is a symbolic link pointing outside of the root. |
| CVE-2026-50329 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50337 | Incorrect type conversion or cast in Windows Notification allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50327 | Heap-based buffer overflow in Windows Media allows an authorized attacker to execute code locally. |
| CVE-2026-50326 | Use after free in Windows Unified Consent System allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50435 | Buffer over-read in Windows Overlay Filter allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50321 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Driver allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50317 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Operating Systems allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50436 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50315 | Null pointer dereference in Windows Image Acquisition allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50314 | Use after free in Microsoft Office allows an unauthorized attacker to execute code locally. |
| CVE-2026-50423 | Improper access control in Windows Kernel allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50422 | Out-of-bounds read in Windows NTFS allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50336 | Heap-based buffer overflow in Windows Media allows an authorized attacker to elevate privileges locally. |
| CVE-2026- | After JavaScript resetting the form, the synchronization process lacks re-entry protection and object lifecycle verification, resulting in the failure of the control pointer during the traversal process. After the pointer fails, it still continues to dereference, causing the application to crash. |

| | |
|---|---|
| 57244 | |
| CVE-2026-50309 | Heap-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally. |
| CVE-2026-15506 | A security vulnerability has been detected in SecureAge CatchPulse up to 10.9.3. The affected element is an unknown function in the library saappctl.sys of the component Driver. Such manipulation leads to heap-based buffer overflow. An attack has to be approached locally. The exploit has been disclosed publicly and may be used. Upgrading to version 10.10.0 is sufficient to fix this issue. You should upgrade the affected component. The vendor was contacted early about this disclosure. |
| CVE-2026-50347 | Heap-based buffer overflow in Windows Data dll allows an unauthorized attacker to execute code locally. |
| CVE-2026-50378 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Key Guard allows an authorized attacker to elevate privileges locally. |
| CVE-2026-57242 | The application opens the PDF, and JavaScript modifies the form. However, the related objects on the page lack complete lifecycle management and null value validation; when the page state changes, the application continuously dereferences invalid objects, eventually leading to a crash. |
| CVE-2026-50346 | Improper authorization in RPC Runtime allows an authorized attacker to elevate privileges locally. |
| CVE-2026-10667 | Zephyr's dynamic kernel-object tracking (kernel/userspace/userspace.c, formerly kernel/userspace.c) maintains a doubly-linked list (obj_list) of dynamically allocated kernel objects. Iteration over this list in k_object_wordlist_foreach() was performed under lists_lock using the SAFE iterator (which caches the next node), but list removal and freeing of nodes was performed under different, disjoint spinlocks: objfree_lock in k_object_free() and obj_lock in unref_check(). On an SMP system, while one CPU iterated obj_list under lists_lock, another CPU could unlink and k_free() the dyn_obj node that the iterator had cached as its next pointer, causing the iterator to dereference freed kernel memory (use-after-free / dangling list traversal). All of the racing operations are reachable from unprivileged user-mode threads via system calls: k_object_alloc/k_object_alloc_size and k_object_release drive removals through unref_check() (under obj_lock), while k_thread_abort and thread creation drive the iteration through k_thread_perms_all_clear()/k_thread_perms_inherit() (under lists_lock). A deprivileged user thread on a CONFIG_SMP + CONFIG_USERSPACE build can therefore corrupt the kernel's object-tracking structures across the userspace security boundary, yielding kernel memory corruption (potential privilege escalation) or a kernel crash (denial of service). The fix removes objfree_lock and serializes every obj_list modification under lists_lock, including holding it across find+remove in k_object_free() and around unref_check() in k_thread_perms_clear(). Affects CONFIG_SMP+CONFIG_USERSPACE+CONFIG_DYNAMIC_OBJECTS configurations; the defect dates to the 2019 spinlockification (commit 8a3d57b6cc6, first released in v1.14.0) and shipped through v4.4.0. |
| CVE-2026-57254 | There is an abnormal annotation within the PDF that is referenced by other objects. When the application parses the PDF, it fails to perform proper type checking, ultimately causing the application to crash. |
| CVE-2026-50386 | Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. |
| CVE-2026-50387 | Stack-based buffer overflow in Windows GDI allows an authorized attacker to elevate privileges locally. |
| CVE-2026-57240 | When the application opens a PDF file and JavaScript deletes the PDF fields, the subsequent logic still uses the old field pointers, resulting in invalid pointer references and causing the application to crash. |
| CVE-2026-50388 | Out-of-bounds read in Windows NTFS allows an unauthorized attacker to execute code locally. |
| CVE-2026-50391 | Improper privilege management in Windows Group Policy allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50373 | Improper access control in Microsoft Windows Search Component allows an authorized attacker to elevate privileges locally. |
| CVE-2026-57238 | After the application opened the PDF, JavaScript deleted the form field object. Subsequently, it attempted to access the invalid object, which caused the application to crash. |
| CVE-2026-57237 | When the application opens a PDF and JavaScript modifies the properties of form fields, it causes the state of the underlying objects referenced by the program to become invalid. Eventually, it reads an illegal memory address, which leads to the crash of the application. |
| CVE-2026-56000 | Local attackers with a X connection able to provide GLX commit to the X server xorg-server before 21.2.24 and xwayland before 24.1.13 could cause a Heap Use After Free, due to CommonMakeCurrent() pointing into potentially reallocated memory. |
| CVE-2026-13129 | When the application opens a PDF file, JavaScript uses the damaged field tree to trigger field traversal, resulting in the program holding an invalid form object when accessing the field property path. Eventually, the application crashes due to reading an invalid pointer. |
| CVE-2026-57256 | When the application opens a PDF and executes JavaScript, it performs abnormal operations on the list box field, and this operation is repeated after the form is reset. During this process, the application failed to adequately verify the validity of the form objects and their internal dictionary pointers, resulting in accessing internal members of invalid or improperly initialized fields. This led to an illegal pointer read, ultimately causing the application to crash. |

| | |
|---|---|
| CVE-2026-50353 | Use after free in Windows DirectX allows an authorized attacker to elevate privileges locally. |
| CVE-2026-57260 | The application opened a PDF file containing an abnormal Unity 3D object. During parsing, the application incorrectly resolved a portion of the abnormal object as a pointer and used it as a valid address, ultimately causing the application to crash. |
| CVE-2026-50344 | Improper authorization in Windows OLE allows an authorized attacker to elevate privileges locally. |
| CVE-2026-13128 | Embedding JavaScript within a PDF file will cause the page to be deleted. Subsequent scripts will continue to access the relevant properties of the document view, eventually leading to the crash of the application. |
| CVE-2026-50343 | Improper privilege management in Microsoft Install Service allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50313 | Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. |
| CVE-2026-55878 | Symfony UX is a JavaScript ecosystem for Symfony. From 2.32.0 before 2.36.1 and from 3.0.0 before 3.2.0, the ux:install console command installs files from a recipe kit by copying paths listed in a copy-files map, and because Path::isRelative() accepts paths like ../../../etc, a crafted or compromised kit can write attacker-controlled content to arbitrary locations or read local files outside the recipe directory. This issue is fixed in versions 2.36.1 and 3.2.0. |
| CVE-2026-57249 | After the application opened the PDF file, the script first reset the annotation status, then triggered the reset form event by additional action. During the re-entry process, the application access invalid objects and crashed. |
| CVE-2026-57250 | When the application opens a PDF and JavaScript resets the form fields, the script re-enters the interface. The underlying native object is damaged, but the application does not perform validation. The function call on the damaged object leads to the application crashing. |
| CVE-2026-50450 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Wireless Wide Area Network Service allows an authorized attacker to elevate privileges locally. |
| CVE-2026-7162 | Successful exploitation of the integer overflow vulnerability could allow an attacker to achieve system-level access to the affected software. |
| CVE-2026-50363 | Heap-based buffer overflow in Windows Push Notifications allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50454 | Relative path traversal in Windows User Interface Core allows an authorized attacker to elevate privileges locally. |
| CVE-2026-57251 | The application opens a PDF, but the cloud-like appearance of the construction process lacks proper setting of an upper limit and consistency checks. Out-of-bounds access to the underlying array is exposed, ultimately leading to a crash of the application. |
| CVE-2026-50407 | Heap-based buffer overflow in Windows Resilient File System (ReFS) allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50306 | Use after free in Windows TCP/IP allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50405 | Insufficient granularity of access control in Windows Filtering Platform (WFP) allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50400 | Stack-based buffer overflow in Windows App Installer allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50417 | Heap-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally. |
| CVE-2026-48368 | Audition is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. |
| CVE-2026-48365 | Audition is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. |
| CVE-2026-50402 | Incorrect conversion between numeric types in Windows NTFS allows an authorized attacker to elevate privileges locally. |
| CVE- | |

| | |
|---|---|
| 2026-48309 | Audition is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. |
| CVE-2026-9492 | The MBStorage DRAM lighting control module within Gigabyte Control Center (GCC) developed by GIGABYTE Technology has an Improper Access Control vulnerability. Authenticated local attackers can send specific IOCTL commands through the driver MyPortIO_x64.sys bundled with the module, thereby arbitrarily reading and writing physical memory and obtaining kernel-level privileges. |
| CVE-2026-50361 | Double free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally. |
| CVE-2026-22927 | Omnissa Workspace ONE® Tunnel for Windows addresses a Local Privilege Escalation Vulnerability. |
| CVE-2026-50362 | Heap-based buffer overflow in Windows Resilient File System (ReFS) allows an unauthorized attacker to execute code locally. |
| CVE-2026-50448 | Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. |
| CVE-2026-47968 | Audition is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. |
| CVE-2026-47642 | Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally. |
| CVE-2026-50412 | Stack-based buffer overflow in Windows NTFS allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50301 | Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally. |
| CVE-2026-50421 | Access of resource using incompatible type ('type confusion') in Windows Connected User Experiences and Telemetry allows an authorized attacker to elevate privileges locally. |
| CVE-2026-57252 | When the application opens a PDF file, during the process of JavaScript deleting pages and removing attachment annotations, it will cause the attachment panel to continue accessing invalid pointers, eventually leading to the application crashing. |
| CVE-2026-47967 | Audition is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. |
| CVE-2026-50440 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Audio Service allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50367 | Incorrect access of indexable resource ('range error') in Windows Sensor Data Service allows an authorized attacker to elevate privileges locally. |
| CVE-2026-57247 | The application re-enters the document structure via field processing and deletes the current page, and then continues using the field objects obtained before deletion, triggering an illegal read and crashing. |
| CVE-2026-50441 | Untrusted pointer dereference in Windows Resilient File System (ReFS) allows an authorized attacker to elevate privileges locally. |
| CVE-2026-57248 | When the application opens a PDF file and JavaScript writes annotation attributes, there is a lack of sufficient object type and argument checks. As a result, due to the damage to the internal structure of the annotations, it causes the application to crash during subsequent release. |
| CVE-2026-50305 | Use after free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50399 | Out-of-bounds read in Windows Kernel allows an authorized attacker to elevate privileges locally. |
| CVE-2026-60002 | ssh in OpenSSH before 10.4 can have a use-after-free when a server changes its host key during a key re-exchange. (This outcome occurs only on the client side.) |
| CVE-2026-33655 | New API is a large language mode (LLM) gateway and artificial intelligence (AI) asset management system. Prior to 0.12.0-alpha.1, the default SSRF protection configuration did not apply IP filtering to hostnames; with ApplyIPFilterForDomain disabled by default, URL validation checked domain allow/block rules but did not resolve a hostname and validate the resolved IP address, allowing authenticated users to configure Webhook, Bark, or Gotify notification URLs that point at an internal or metadata IP address. This issue is fixed in version 0.12.0-alpha.1. |
| | |

| | |
|---|---|
| CVE-2026-55874 | SeaweedFS is a distributed storage system. Prior to 4.34, the S3 API gateway does not reject dot-dot path segments in the X-Amz-Copy-Source header used by CopyObject and UploadPartCopy, allowing an authenticated identity scoped to one bucket to read objects from other buckets through server-side copy. This issue is fixed in version 4.34. |
| CVE-2026-14373 | HashiCorp Nomad and Nomad Enterprise did not enforce the allow_privileged restriction for the Docker task driver's host namespace mode options. This may allow an authenticated job submitter to run a container in a host namespace and access information belonging to the host or to other workloads on the same client. This vulnerability, CVE-2026-14373, is fixed in Nomad Community Edition 2.0.4 and Nomad Enterprise 2.0.4, 1.11.8, and 1.10.14. |
| CVE-2026-56689 | Dell PowerFlex Manager, Version prior to 5.1.0.1, contain(s) an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure. |
| CVE-2026-55659 | Grist is spreadsheet software using Python as its formula language. Prior to 1.7.15, several server-rendered Grist pages embedded user-controlled values into the page and into inline scripts without fully escaping them, allowing cross-site scripting. On the main application page, a document's name or description, set by a document editor, is rendered into the page that other users load when opening the document. On the OAuth2 end-of-flow page, the openerOrigin request parameter was reflected back into the served page. Injected script runs in the victim's Grist origin and can act through the authenticated session, reading or modifying data and changing sharing settings and access rules. A document editor could therefore escalate to owner-level access. This issue is fixed in version 1.7.15. |
| CVE-2026-55516 | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, PATCH or PUT /api/v1/maintenances/{maintenance_id} checks access to the current maintenance record and asset but then fills attacker-controlled fields including asset_id without re-authorizing the newly supplied asset, allowing an authorized user to move a maintenance record onto an asset outside their company scope. This issue is fixed in version 8.6.2. |
| CVE-2026-14903 | Path traversal in Ivanti  Xtraction before version 2026.2.1 allows a remote authenticated attacker to read arbitrary files outside the web root. |
| CVE-2026-58207 | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.3 and 2.12.12, a client able to send account-scoped connection monitoring requests could crash the server by supplying Connz pagination Offset and Limit values that overflowed internal arithmetic before the response window was safely bounded. This issue is fixed in versions 2.14.3 and 2.12.12. |
| CVE-2026-59216 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.10.0, get_event_call delivered execute:python and execute:tool Socket.IO events to a client-supplied session_id after checking only that the session was connected, allowing authenticated users who learned another socket ID through ydoc:document:join to run code interpreter Python or tools in that user session. This issue is fixed in version 0.10.0. |
| CVE-2026-57212 | RabbitMQ is a messaging and streaming broker. Prior to 3.13.14, 4.0.19, 4.1.10, and 4.2.5, the rabbitmq_management HTTP API accepts oversized valid JSON bodies on with_decode and direct_request paths because read_complete_body checks the accumulated size before the final chunk but not the final combined size. This issue is fixed in versions 3.13.14, 4.0.19, 4.1.10, and 4.2.5. |
| CVE-2026-55431 | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, `coder open app` opens external workspace-app URLs without validating the scheme or host. When an external app URL contains the `$SESSION_TOKEN` placeholder the CLI replaces it with the user's real session token before handing the URL to the OS open handler. Practical exploitation requires the victim to run `coder open app` against a workspace whose external app definition the attacker controls. Only a malicious template author can control external app URLs. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 applies a URL-scheme allowlist in the CLI and limits `$SESSION_TOKEN` substitution to trusted destinations like the web frontend. As a workaround, avoid running `coder open app` for untrusted workspaces. |
| CVE-2026-59832 | SiYuan is an open-source personal knowledge management system. Prior to 3.7.1, the /snippets/*filepath route handler serveSnippets in kernel/server/serve.go joins a single-decoded request path with the snippets directory without subpath containment or sensitive-path checks, allowing an authenticated request such as /snippets/%2e%2e/%2e%2e/conf/conf.json to read workspace secrets and the document database. This issue is fixed in versions 3.7.1. |
| CVE-2026-55208 | Pimcore Studio Backend Bundle is the backend bundle for Pimcore Studio. Prior to 2025.4.6 and 2026.1.6, an authenticated user can extract the admin password hash and other database content through time-based blind SQL injection in the DateFilter column key parameter. The POST /pimcore-studio/api/website-settings endpoint and other listing endpoints accept a columnFilters array where the key field is interpolated directly into SQL with manual backtick wrapping, allowing a backtick character to break out of quoting and append arbitrary SQL such as SLEEP() and IF() subqueries. This issue is fixed in versions 2025.4.6 and 2026.1.6. |
| CVE-2026-59221 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.6 before 0.10.0, _sanitize_proxy_path in backend/open_webui/routers/terminals.py decoded proxy paths only eight times, allowing a nine-times percent-encoded ../ traversal value to pass normalization checks and be decoded by the upstream terminal server. This issue is fixed in version 0.10.0. |
| CVE-2026-58233 | SAP Change and Transport System Attach Tool (ctsattach) allows an authenticated attacker to supply a specially crafted archive file which, when processed by the application's library, can trigger insecure deserialization and lead to remote code execution (RCE) on the system. Successful exploitation requires a victim to process the malicious archive, enabling the attacker to execute the RCE and extract sensitive information and gain control over the system and its processes. This vulnerability has a high impact on confidentiality and integrity of the data, with a low impact on the availability of the system. |
| CVE-2026-55405 | LangChain4j is a Java library for building LLM-powered applications on the JVM. Prior to 1.2.1-beta8, 1.5.1-beta11, 1.11.8-beta19, and 1.16.3-beta26, the MariaDB and pgvector embedding stores build metadata-filter SQL by string-concatenating filter keys, and in MariaDB string values, directly into the query without adequate escaping. A crafted metadata key in EmbeddingSearchRequest.filter() can break out of its SQL context and inject arbitrary SQL into the statements executed by the stores' search and removeAll(Filter) operations, enabling blind data exfiltration, denial of service via sleep functions, and deletion of arbitrary rows through removeAll(Filter). This issue is fixed in langchain4j-mariadb and langchain4j-pgvector versions 1.2.1-beta8, 1.5.1-beta11, 1.11.8-beta19, and 1.16.3-beta26. |
| CVE-2026-62185 | Argo CD Helm Chart before 10.0.0 fails to install network policies by default, allowing any pod on a cluster to access repo-server and other Argo APIs. Attackers can exploit this unrestricted network access through combined attacks to achieve cluster compromise and remote code execution. |
| CVE-2026-62186 | OpenClaw versions before 2026.6.8 contain an authorization bypass vulnerability in OpenAI-compatible HTTP model overrides that allows lower-trust callers to perform actions requiring stronger authorization checks. Attackers can exploit misconfigured input paths to bypass admin authorization policies and execute restricted operations. |
| CVE-2026-57773 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Zorem Advanced Shipment Tracking for WooCommerce woo-advanced-shipment-tracking allows Blind SQL Injection.This issue affects Advanced Shipment Tracking for WooCommerce: from n/a through <= 4.0. |
| CVE-2026-61955 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Hannan گرویتی فرم فارسی  persian-gravity-forms allows Blind SQL Injection.This issue affects گرویتی فرم فارسی : from n/a through <= 3.0.2. |
| CVE- | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, a run of closed tilde, equals-sign, or caret marker pairs around a character causes |

| | |
|---|---|
| 2026-59922 | quadratic work in src/mistune/plugins/formatting.py when the strikethrough, mark, or insert plugin scans for matching markers from each possible start position, allowing denial of service through CPU exhaustion. This issue is fixed in version 3.3.0. |
| CVE-2026-59873 | node-tar is a tar archive manipulation library for Node.js. Prior to 7.5.19, node-tar does not enforce hard upper bounds on total decompressed data, entry counts, or decompression ratio in extraction and parsing paths such as src/extract.ts, allowing a small crafted gzip bomb to exhaust disk space and CPU. This issue is fixed in version 7.5.19. |
| CVE-2026-59205 | Pillow is a Python imaging library. Prior to 12.3.0, Pillow's ImageCms.ImageCmsTransform.apply(im, imOut) API can trigger controlled native heap corruption when the caller supplies an output image whose mode does not match the transform's declared output mode. This issue is fixed in version 12.3.0. |
| CVE-2026-59720 | Hoppscotch is an open source API development ecosystem. Prior to 2026.6.0, mock server creation in mock-server.service.ts does not persist the isPublic input field while schema.prisma defaults isPublic to true, causing mock servers linked to private collections to be publicly accessible without authentication and potentially expose sensitive API data. This issue is fixed in version 2026.6.0. |
| CVE-2026-40006 | Memory Allocation with Excessive Size Value, Allocation of Resources Without Limits or Throttling, Missing Authentication for Critical Function vulnerability in Apache IoTDB. When pipe_air_gap_receiver_enabled=true, the IoTDB AirGap pipe receiver accepts raw TCP connections on port 9780 with no authentication. The readLength method reads an attacker-controlled 32-bit integer from the socket and readData passes it directly to new byte[length] with no upper-bound check. An unauthenticated attacker can cause the JVM to attempt an allocation of up to 2,147,483,647 bytes per connection, exhausting heap memory and crashing or severely degrading the DataNode process. This issue affects Apache IoTDB: from 1.0.0 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue. |
| CVE-2026-59874 | node-tar is a tar archive manipulation library for Node.js. Prior to 7.5.18, tar.replace accepts a checksum-valid tar header with a negative base-256 encoded entry size, causing the archive scanner to make no progress while repeatedly parsing the same header. This issue is fixed in version 7.5.18. |
| CVE-2026-59880 | Immutable.js provides many Persistent Immutable data structures. Prior to 4.3.9 and 5.1.8, Immutable.Map and Immutable.Set keep keys that share the same 32-bit hash in a HashCollisionNode collision bucket that is scanned linearly, allowing an attacker who controls keys inserted into a Map, such as through Immutable.Map(obj), Immutable.fromJS(obj), state.merge(userObject), or mergeDeep, to craft many colliding keys and degrade insertion and lookup to consume disproportionate CPU. This issue is fixed in versions 4.3.9 and 5.1.8. |
| CVE-2026-59887 | linkify-it is a links recognition library with full Unicode support. Prior to 5.0.2, the mailto: schema validator used by .test() and .match() can be invoked at every mailto: occurrence and scan the remaining input through src_email_name in lib/re.mjs, causing O(n^2) CPU consumption on crafted user text. This issue is fixed in version 5.0.2. |
| CVE-2026-40454 | Out-of-bounds Read, Improper Input Validation vulnerability in Apache IoTDB C++ client. Out-of-bounds reads in IoTDB C++ client TsBlock deserializer crash client process on malformed server data. This issue affects Apache IoTDB C++ client: from 1.3.5 before 1.3.8, from 2.0.5 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue. |
| CVE-2026-50379 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Media allows an authorized attacker to elevate privileges over a network. |
| CVE-2026-59879 | Immutable.js provides many Persistent Immutable data structures. Prior to 4.3.9 and 5.1.8, List#set, List#setSize, List#setIn, List#updateIn, and the functional set, setIn, and updateIn mishandle an index or size in the range 2 ** 30 to 2 ** 31 in setListBounds in src/List.js, causing an empty List to enter an uncatchable infinite loop, a populated List to allocate without bound until process abort, or setSize to silently wrap large values. This issue is fixed in versions 4.3.9 and 5.1.8. |
| CVE-2026-40007 | Uncontrolled Recursion, Uncontrolled Resource Consumption vulnerability in Apache IoTDB. When pipe_air_gap_receiver_enabled=true, the IoTDB AirGap receiver's readLength method calls itself recursively each time it recognises the E-language prefix in socket data, with no depth limit. An unauthenticated attacker can send a stream of repeated E-language prefixes that drives the recursion arbitrarily deep, exhausting the receiver thread's JVM stack and raising StackOverflowError. This issue affects Apache IoTDB: from 1.0.0 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue. |
| CVE-2026-0287 | Multiple denial of service vulnerabilities in Palo Alto Networks PAN-OS® software allow an unauthenticated attacker with network access to cause a denial of service (DoS) condition by sending specially crafted network traffic to or through a dataplane interface. Repeated attempts to trigger this condition result in the firewall entering maintenance mode. Panorama is not impacted by these vulnerabilities. |
| CVE-2026-59841 | A improper restriction of communication channel to intended endpoints vulnerability in Fortinet FortiSIEMWindowsAgent 7.4.0 through 7.4.1 may allow attacker to escalation of privilege via <insert attack vector here> |
| CVE-2026-50653 | Loop with unreachable exit condition ('infinite loop') in Azure Active Directory allows an unauthorized attacker to deny service over a network. |
| CVE-2026-50652 | Deserialization of untrusted data in Azure Active Directory allows an unauthorized attacker to deny service over a network. |
| CVE-2026-29008 | U-Boot through 2026.04-rc3 contains an integer underflow vulnerability in the tcp_rx_state_machine() function (net/tcp.c) that allows a network-adjacent attacker to crash the bootloader by sending a malformed TCP SYN+ACK packet with a manipulated data offset field causing payload_len to become negative. When the TCP_SYN_SENT handler calls tcp_rx_user_data() without invoking tcp_seg_in_wnd() validation, the negative payload_len is implicitly converted to a large unsigned integer (e.g., 0xFFFFFFD8) and passed to memcpy() in store_block(), causing an immediate crash that prevents device boot and may enable memory corruption when CONFIG_LMB is disabled. |
| CVE-2026-50506 | Allocation of resources without limits or throttling in ASP.NET Core allows an unauthorized attacker to deny service over a network. |
| CVE-2025-63579 | Unauthorized use of Kyocera printers, allows all information stored in the Kyocera address book to be exported. The security measure that encrypts incoming data ian be bypassed with this vulnerability, allowing encrypted data to be decrypted. Passwords and other sensitive information can be obtained. This affects Kyocera Command Center RX TASKalfa 2552ci, TASKalfa 3252ci, TASKalfa 2553ci, TASKalfa 3253ci, TASKalfa 3554ci, TASKalfa 4052ci, TASKalfa 5052ci, TASKalfa 6052ci, TASKalfa 7052ci, TASKalfa 8052ci, TASKalfa 7353ci, TASKalfa 8353ci, TASKalfa 2554ci, TASKalfa 3254ci, TASKalfa 505. |
| CVE-2026-26396 | OpenBMB XAgent v1.0.0 and before is vulnerable to path traversal in the file() function in XAgent/XAgentServer/application/routers/workspace.py. The input parameter “filename” is user-controllable and is concatenated into the file path to be read without proper validation, leading to a directory traversal vulnerability that may result in sensitive information disclosure. |
| | OpenTelemetry JavaScript is the OpenTelemetry JavaScript client. Prior to 2.9.0, @opentelemetry/propagator-jaeger decodes incoming uber-trace-id and uberctx-* |

| | |
|---|---|
| CVE-2026-59892 | HTTP header values with decodeURIComponent() without handling decode errors, allowing an unauthenticated remote attacker to send a malformed percent-encoded value that throws an uncaught URIError and terminates a Node.js process using JaegerPropagator as the active propagator. This issue is fixed in version 2.9.0. |
| CVE-2026-13347 | The Hide My WP Lite plugin for WordPress is vulnerable to Arbitrary File Read in versions up to and including 1.3 via the he_wrapper_js and he_wrapper_css query parameters processed by the elementor_assets_filter() function. This is due to the function concatenating user-supplied input directly onto ABSPATH and passing the result to file_get_contents() without any path traversal validation, allow-list, realpath containment, or extension check; the result is then echoed in the HTTP response. Although the output is passed through wp_kses_post(), that function only filters HTML tags and does not prevent disclosure of arbitrary file contents. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the affected site's server (such as wp-config). Note: The exploit requires the Elementor plugin and the 'Hide Elementor' feature to be enabled. |
| CVE-2026-59836 | A improper certificate validation vulnerability in Fortinet FortiClientEMS 7.4.3 through 7.4.5, FortiClientEMS 7.4.0 through 7.4.1, FortiClientEMS 7.2 all versions may allow attacker to information disclosure via <insert attack vector here> |
| CVE-2026-54695 | Pipecat is an open-source Python framework for building real-time voice and multimodal conversational agents. Prior to 1.4.0, the pipecat development runner registers a /ws WebSocket endpoint for telephony testing that accepts connections without authentication, reads an attacker-supplied callSid from a Twilio stream-start handshake in src/pipecat/runner/utils.py, and passes it to TwilioFrameSerializer so the server can issue an authenticated Twilio REST API hang-up request with the server operator's credentials; equivalent unauthenticated call-control sinks exist for Telnyx and Plivo. This issue is fixed in version 1.4.0. |
| CVE-2026-12685 | The EscortWP escortwp WordPress theme through 3.6.2 was distributed with a vendor-authored, obfuscated backdoor that lets an unauthenticated attacker who supplies a hard-coded, per-build key permanently delete all of the site's content, and that covertly transmits the site URL, administrator email address, and license key to a third-party server. |
| CVE-2025-3110 | OpenVPN Access Server 2.7.2 through 3.1.0 accepts bare line-feed sequences inside HTTP header values, allowing remote attackers to perform HTTP request smuggling when deployed behind a reverse proxy |
| CVE-2026-40452 | Incorrect Authorization, Improper Access Control vulnerability in Apache IoTDB. Authorization bypass in /rest/v2/fastLastQuery exposes last-value data to unauthorized authenticated users. This issue affects Apache IoTDB: from 1.3.5 before 1.3.8, from 2.0.5 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue. |
| CVE-2026-61458 | PasswordPusher before 2.9.2 contains a brute-force vulnerability in the POST /p/:token/access endpoint that lacks route-specific rate limiting and per-push lockout mechanisms. Attackers who know a push token can systematically guess passphrases at 120 attempts per minute without triggering any push-level defense, making short or dictionary-derived passphrases practically recoverable within hours or days. |
| CVE-2026-59869 | js-yaml is a JavaScript YAML parser and dumper. From 3.0.0 before 3.15.0 and from 4.0.0 before 4.3.0, js-yaml can spend quadratic CPU time parsing a document whose size grows only linearly when a chain of mappings uses merge keys where each mapping merges the previous one. This issue is fixed in versions 3.15.0 and 4.3.0. |
| CVE-2026-49788 | Allocation of resources without limits or throttling in HTTP/2 allows an unauthorized attacker to deny service over a network. |
| CVE-2026-14165 | An Authorization Bypass Through User-Controlled Key vulnerability affecting Tuleap Enterprise Edition from 17.0 through 17.5 could allow an attacker to access data of other users without authorization. |
| CVE-2026-10708 | This vulnerability enables large-scale data harvesting without requiring app-specific secrets. A single request to a minimal leaderboard component may return user records containing emails, UUIDs, and custom fields. The combination of wildcard CORS behavior, long-lived twenty-day JWTs, and the absence of token revocation allows attackers to gather sensitive personal information from any Adalo application. |
| CVE-2026-10706 | In Adalo’s no-code app builder, (Versions 1 and 2) the attackers may extract full user records and correlate user behavior across multiple applications via dbId enumeration. The platform does not implement data minimization, privacy by design, or implement appropriate technical safeguards, allowing sensitive information to be exposed to unauthorized parties. |
| CVE-2026-10699 | Missing release of memory after effective lifetime vulnerability in Progress MOVEit Transfer (Custom Reports modules). This issue affects MOVEit Transfer: from 2025.0.0 before 2025.0.8, from 2025.1.0 before 2025.1.4, from 2026.0.0 before 2026.0.1. |
| CVE-2026-15291 | The Chat Help – Click to Chat Button & Form plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.1.3 via the REST API endpoints /wp-json/chat-help/v1/leads and /wp-json/chat-help/v1/leads/{id}. This is due to the plugin not performing any authentication and authorization checks. This makes it possible for unauthenticated attackers to extract sensitive data including customer names, email addresses, phone numbers, WhatsApp messages, complete geolocation data (IP addresses, city, country, ISP, coordinates), device fingerprinting information (browser, OS, screen resolution), and WordPress account credentials (user IDs, usernames, emails, names) for logged-in users who submit forms. |
| CVE-2026-55233 | OpenResty is a high performance web platform. From 1.29.2.1 to before 1.29.2.5, an out-of-bounds write vulnerability exists in the upstream PROXY protocol v2 implementation. When OpenResty is configured to send PROXY protocol version 2 headers to upstream servers, constructing the header in the stream proxy protocol v2 patch can write beyond the bounds of the allocated buffer, causing the worker process to crash and resulting in a denial of service. Only configurations that explicitly enable PROXY protocol v2 for upstream connections are impacted. This issue is fixed in version 1.29.2.5. |
| CVE-2026-15290 | The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to blind SQL Injection via the search parameter in all versions up to, and including, 2.10.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This vulnerability was partially patched in version 2.9.2 when initially addressing CVE-2025-0308. |
| CVE-2026-15053 | Tanium addressed a denial of service vulnerability in Tanium Server. |
| CVE-2026-59834 | SiYuan is an open-source personal knowledge management system. Prior to 3.7.1, the block search endpoint POST /api/search/fullTextSearchBlock concatenates attacker-controlled paths values into SQL predicates used by non-SQL search modes, allowing an unauthenticated publish visitor to inject a UNION SELECT and return rows from hidden documents by projecting an allowed visible box and path. This issue is fixed in versions 3.7.1. |
| CVE-2026-55229 | Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.34.0, Gotenberg's /forms/libreoffice/convert endpoint allows a specially crafted document to cause LibreOffice to automatically retrieve external HTTP(S) resources and local file resources during document conversion, enabling blind SSRF and limited local file disclosure via linked image resource loading. This issue is fixed in version 8.34.0. |

| | |
|---|---|
| CVE-2026-49787 | Allocation of resources without limits or throttling in Windows HTTP.sys allows an unauthorized attacker to deny service over a network. |
| CVE-2026-50424 | Untrusted pointer dereference in Windows Domain Controller allows an unauthorized attacker to deny service over a network. |
| CVE-2026-55213 | h2o is an HTTP server with support for HTTP/1.x, HTTP/2 and HTTP/3. Prior to commit edd7a120bfc4af11ac0cbebce2a43cc1f93f9af1, when h2o processes a QPACK instruction sent from the peer over HTTP/3, lib/http3/qpack.c might allocate an on-stack buffer as large as approximately 800 KB by calling alloca, which exceeds the default pthread stack size used by musl libc and causes the h2o server to crash with a segmentation fault while touching the guard page. This issue is fixed in commit edd7a120bfc4af11ac0cbebce2a43cc1f93f9af1. |
| CVE-2026-58656 | Grav API plugin before v1.0.0-rc.16 accepts JWT tokens via the ?token= URL query parameter and responds with Access-Control-Allow-Origin: *, allowing unauthenticated attackers to make fully authenticated cross-origin API requests from any malicious website. Attackers who obtain a leaked JWT token from access logs, proxy logs, browser history, or Referrer headers can create persistent backdoor super-admin accounts and exfiltrate sensitive configuration and user data. |
| CVE-2026-15288 | The SureForms – Drag and Drop Form Builder for WordPress plugin for WordPress is vulnerable to Improper Input Validation in all versions up to, and including, 2.2.1. This is due to the plugin accepting the payment amount directly from user-controlled POST data in the 'create_payment_intent' and 'create_subscription_intent' functions without validating it against the form's configured price. This makes it possible for unauthenticated attackers to modify the payment amount to any arbitrary value when submitting a Stripe payment form, potentially purchasing products or services at significantly reduced prices. |
| CVE-2026-44840 | Dgraph is an open source distributed GraphQL database. Prior to version 25.3.4, the `checkUserPassword` GraphQL query in Dgraph is vulnerable to DQL (Dgraph Query Language) injection. User-supplied password values are interpolated directly into a DQL `checkpwd()` query via `fmt.Sprintf` without any escaping or parameterization. An attacker can inject a password containing a double-quote character to break out of the DQL string literal and append arbitrary DQL query blocks. Version 25.3.4 patches the issue. |
| CVE-2026-55827 | FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.27.1, FreeRDP clients launched with the non-default /cache:codec:rfx option pass desktop stride and height to RemoteFX decoding for Cache Bitmap V3 data while allocating bitmap->data only for the smaller DstWidth and DstHeight in gdi_Bitmap_Decompress, allowing a malicious RDP server to trigger a heap out-of-bounds write with attacker-controlled offset and content. This issue is fixed in version 3.27.1. |
| CVE-2026-49181 | Integer underflow (wrap or wraparound) in Windows DHCP Client allows an unauthorized attacker to elevate privileges over a network. |
| CVE-2026-50411 | Stack-based buffer overflow in Active Directory Federation Services (AD FS) allows an unauthorized attacker to deny service over a network. |
| CVE-2026-53482 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an Integer overflow or wraparound vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to denial of service. |
| CVE-2026-49171 | Use after free in Microsoft Windows Speech allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50414 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Media allows an authorized attacker to elevate privileges over a network. |
| CVE-2026-57026 | An Improper Validation of Syntactic Correctness of Input vulnerability in the SIP plugin of Juniper Networks Junos OS on MX Series with SPC3 and SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS).If the SIP ALG is enabled on an affected device, the processing of a malformed SIP invite packet will cause a flow processing daemon (flowd) crash and restart. This leads to a complete service outage until the system has automatically recovered. This issue affects Junos OS on MX Series with SPC3 and SRX Series: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S5, * 24.4 versions before 24.4R2-S4, * 25.2 versions before 25.2R2, * 25.4 versions before 25.4R1-S2. |
| CVE-2026-5356 | The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Improper Input Validation in all versions up to, and including, 5.4.0. This is due to the plugin's Stripe Connect payment processor accepting a client-supplied PaymentIntent ID. This makes it possible for unauthenticated attackers to pay an arbitrary amount by supplying a previously succeeded PaymentIntent token. |
| CVE-2026-59725 | Socket.IO enables bidirectional and low-latency communication for every platform. From 4.1.0 before 6.6.7, Engine.IO protocol v4 polling transport does not properly close the HTTP response for invalid binary POST requests with Content-Type: application/octet-stream, allowing an unauthenticated attacker to exhaust server-side connections and sockets. This issue is fixed in version 6.6.7. |
| CVE-2026-45646 | Allocation of resources without limits or throttling in ASP.NET Core allows an unauthorized attacker to deny service over a network. |
| CVE-2026-59724 | Socket.IO enables bidirectional and low-latency communication for every platform. From 6.5.0 before 6.6.7, Engine.IO servers with WebTransport enabled can resolve a crafted session ID such as __proto__ through an inherited property of the clients object during WebTransport upgrade handling, causing a TypeError and denial of service. This issue is fixed in version 6.6.7. |
| CVE-2026-51926 | An issue in docuForm GmbH FSM Client v.11.11c allows a remote attacker to obtain sensitive information via the login.php component. A vulnerability was identified in the authentication mechanism that allows user enumeration through the login interface. An attacker can differentiate between valid and invalid usernames based on variations in server responses. This information can be leveraged to identify existing accounts and facilitate further attacks, including brute-force or credential stuffing. |
| CVE-2026-40378 | Memory allocation with excessive size value in Windows Local Security Authority Subsystem Service (LSASS) allows an unauthorized attacker to deny service over a network. |
| CVE-2026-15271 | A security vulnerability has been detected in TOTOLINK A3000RU, A3100R, A950RG, AC1200T10, CP450, CS185R_T10 and EX200 up to 20260906. Affected by this issue is some unknown functionality of the file /etc/boa/boa.conf of the component Web Interface. The manipulation leads to least privilege violation. The attack may be initiated remotely. The attack's complexity is rated as high. The exploitation is known to be difficult. |

| | |
|---|---|
| CVE-2026-15574 | A flaw was found in the vllm-orchestrator-gateway component. The system's production binary logs all incoming authorization headers and full chat payloads, which may contain personally identifiable information (PII) and secrets, to persistent logs. This sensitive data, including bearer tokens and chat content, can be accessed by any user with logging privileges. This vulnerability leads to information disclosure, potentially allowing an attacker to harvest credentials and sensitive conversation content. |
| CVE-2026-39042 | An issue in MikroTlk (SIA Mikrotikls, Latvia) RouterOS 7.21.x before v.7.21.4 and 7.22.x before v.7.22.2 allows a remote attacker to cause a denial of service via the unflatten() function in libumsg.so. |
| CVE-2026-59703 | repomix contains a local file inclusion vulnerability in the git clone endpoint that allows unauthenticated attackers to read arbitrary local git repositories. The isValidRemoteValue function in src/core/git/gitRemoteParse.ts fails to block file:// URLs, permitting attackers to supply file:// scheme URLs that bypass validation and are passed directly to git clone, enabling unauthorized access to all tracked file contents on the server filesystem. |
| CVE-2026-38076 | An integer overflow in the jbig2_arith_iaid_ctx_new() function of Artifex commit cc37d0 allows attackers to cause a Denial of Service (DoS) via a crafted input. |
| CVE-2026-51539 | A Denial of Service (DoS) vulnerability exists in the receive loop of libmodbus 3.1.12 when running on Windows. The issue stems from improper timeout management during network read operations. |
| CVE-2026-39246 | decompress before 4.2.2 allows arbitrary symlink creation during archive extraction. When processing symlink entries (type === 'symlink'), the x.linkname field from the archive is passed directly to fs.symlink() without validation (index.js line 121). The preventWritingThroughSymlink check on line 98 only applies to file entries, not symlink creation. An attacker can craft an archive with symlink entries pointing to sensitive files outside the extraction directory (e.g., /etc/passwd), enabling information disclosure when the application reads the extracted contents. |
| CVE-2026-45788 | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, secure uploads could be exposed by pull_hotlinked_images when an attacker knew the secured upload URL and the secure_uploads site setting was enabled. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5. |
| CVE-2026-57023 | An Improper Validation of Specified Quantity in Input vulnerability in the TCP proxy plugin of Juniper Networks Junos OS on MX Series with SPC3, and SRX Series allows an unauthenticated, network-based attacker to cause a complete Denial of Service (DoS). When TCP proxy is engaged in a flow session, to support ALGs, Advanced Anti-Malware, ICAP or UTM, a TCP packet with specifically malformed TCP header will cause flow processing daemon (flowd) to crash and restart. This causes a complete service outage until the system has automatically recovered. This issue affects Junos OS on MX with SPC3, and SRX Series: * 23.4 versions before 23.4R2-S7, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S3, * 25.2 versions before 25.2R2. This issue does not affect releases before 23.4R1. |
| CVE-2026-50368 | Stack-based buffer overflow in Active Directory Federation Services allows an unauthorized attacker to deny service over a network. |
| CVE-2026-49256 | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, restricted tag and tag-group names attached to publicly readable categories as allowed_tags, allowed_tag_groups, or required tag groups could leak to anonymous and unauthorized users through category and group endpoints. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5. |
| CVE-2026-57220 | RabbitMQ is a messaging and streaming broker. Prior to 4.2.6, the RabbitMQ stream listener does not enforce the configured stream frame-size limit while assembling frames during authentication and before Tune negotiation, allowing an unauthenticated remote client to declare oversized frame lengths and consume broker memory in rabbit_stream_core. This issue is fixed in version 4.2.6. |
| CVE-2026-49147 | App::Ack versions through 3.10.0 for Perl print unsanitised terminal escape sequences from filenames in several output modes. When ack prints a filename whose basename contains terminal control bytes such as ANSI escape sequences, those bytes reach the terminal unchanged. Version 3.10.0 added a _safe_filename helper that sanitises the filenames printed by -f, -g, the colored match heading, and per-match lines, but the --show-types, -l/-L, and -c paths still emit the raw filename. A file whose name embeds cursor-movement or color escapes can overwrite or recolor earlier terminal output, or be passed unchanged to a downstream consumer. |
| CVE-2026-6230 | The Tainacan plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'geoquery' parameter in all versions up to and including 1.0.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. |
| CVE-2026-49146 | App::Ack versions before 3.10.0 for Perl allow memory exhaustion via an unbounded context value in a project .ackrc. ack searches up the directory hierarchy from the current directory for a project .ackrc and loads its options. The -B and -C context options accepted any positive integer, and ack sized the before-context buffer to that value, so a project .ackrc setting --before-context=100000000 made ack allocate a buffer of 100 million elements. A project .ackrc committed to an untrusted repository can abort ack with an out-of-memory condition. |
| CVE-2026-57219 | RabbitMQ is a messaging and streaming broker. Prior to 3.13.15, 4.0.20, 4.1.11, and 4.2.6, the obsolete GET /api/auth endpoint can disclose the OAuth 2 client secret on RabbitMQ installations configured with management.oauth_client_secret, exposing credentials to unauthenticated callers when the management plugin and that OAuth configuration are enabled. This issue is fixed in versions 3.13.15, 4.0.20, 4.1.11, and 4.2.6. |
| CVE-2026-49145 | App::Ack versions through 3.10.0 for Perl read arbitrary files via --files-from in a project .ackrc. ack searches up the directory hierarchy from the current directory for a project .ackrc and loads its options. The project-source option blocklist in App::Ack::ConfigLoader does not include --files-from, so a project .ackrc can set it to a path whose listed files ack then reads and searches. Version 3.10.0 added --follow to the blocklist; --files-from remains accepted. A project .ackrc committed to an untrusted repository can make ack read files outside the project and print their matching lines. |
| CVE-2026-6854 | The My Calendar – Accessible Event Manager plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'mc_auth' parameter in all versions up to, and including, 3.7.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. |
| CVE-2026-62184 | luci-app-banip contains a log parsing vulnerability where the awk-based parser extracts the first IPv4 address from log lines regardless of field position, allowing attackers to inject arbitrary IPs via attacker-controlled fields like usernames. An unauthenticated remote attacker can inject an IP address into the login username field, causing banIP to block the wrong target while the real attacker remains unblocked. |
| CVE-2026-55420 | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, under certain non-default configurations, processing of PDF uploads could be exploited to obtain RCE on the server. This issue is patched in 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5. |
| CVE-2026- | A weakness has been identified in D-link DIR-823G 1.0.2B05_20181207. Affected by this vulnerability is an unknown functionality of the file /etc/boa/boa.conf of the component Web Interface. Executing a manipulation can lead to least privilege violation. The attack can be launched remotely. The attack requires a high |

| | |
|---|---|
| 15270 | level of complexity. The exploitation appears to be difficult. The exploit has been made available to the public and could be used for attacks. |
| CVE-2026-50695 | Stack-based buffer overflow in Active Directory Federation Services allows an unauthorized attacker to deny service over a network. |
| CVE-2026-15338 | The LA-Studio Element Kit for Elementor plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.6.1 via the get_type_template function. This makes it possible for authenticated attackers, with contributor-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included. The wp_normalize_path function used in get_template only normalizes directory separators and does not resolve or reject path traversal sequences, while the extension check is trivially bypassed because the caller already appends the required extension to the traversal payload. |
| CVE-2026-50304 | Stack-based buffer overflow in Active Directory Federation Services allows an unauthorized attacker to deny service over a network. |
| CVE-2026-14244 | The Jssor Slider by jssor.com plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 3.1.24 via the 'url' parameter parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. |
| CVE-2026-47840 | A network attacker positioned between UAA and its LDAP directory can impersonate the directory using any certificate from any trusted CA, then harvest the LDAP bind password and every end-user password sent during simple-bind authentication, and return forged group memberships that grant themselves admin scopes. This affects every deployment that authenticates users against LDAP over StartTLS. Affected versions: UAA versions prior to v78.13.0; Cf-deployment versions prior to v56.2.0. |
| CVE-2026-49866 | libp2p is a JavaScript Implementation of libp2p networking stack. Prior to 16.0.0, @libp2p/gossipsub defaultDecodeRpcLimits set maxIhaveMessageIDs and maxIwantMessageIDs to Infinity, allowing oversized IHAVE and IWANT control message arrays in message/decodeRpc.ts and gossipsub.ts to synchronously iterate roughly 180,000 message IDs per 4 MB frame and block the Node.js event loop. This issue is fixed in version 16.0.0. |
| CVE-2026-9842 | The Backstage - Customizer Demo Access plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.4.2. This is due to the plugin assigning the `manage_options` capability to the `backstage_customizer_user` demo role, which is more permissive than necessary for Customizer-only demo access. This makes it possible for unauthenticated attackers to navigate beyond the Customizer and update arbitrary WordPress options such as `default_role`, leading to privilege escalation. |
| CVE-2026-56279 | Capgo before 12.128.2 contains an information disclosure vulnerability in the get_orgs_v7(userid) RPC function that remains publicly invokable despite intended private access controls. Unauthenticated attackers can supply arbitrary user UUIDs to retrieve foreign users' organization membership, roles, management emails, and billing metadata. |
| CVE-2026-15167 | DBS Etherwatch file parser crash in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service |
| CVE-2026-55687 | ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. Versions 6.0.1, 5.5.4, 5.4.4, 5.3.5, and possibly prior contain an out-of-bounds write in jpeg_parse_dqt_marker() in components/esp_driver_jpeg/jpeg_parse_marker.c because the attacker-controlled DQT marker Tq nibble is used as an index into the qt_tbl array without validating that it is in the range 0..3, allowing malformed JPEG input to corrupt stack memory and reliably trigger a denial of service. This issue is fixed in version 6.0.2 and is expected to be fixed in versions 5.5.5, 5.4.5, and 5.3.6. |
| CVE-2026-38059 | The iDirect iQ200 exposes the /api/identity and /api/ REST API endpoints without authentication. An unauthenticated attacker with network access can retrieve sensitive device information including the serial number, Device ID (DID), Terminal Private Key identifier (TPK), MAC address, and exact firmware version. The DID and TPK are used for satellite network authentication in the iDirect platform, potentially enabling terminal impersonation and network reconnaissance. |
| CVE-2026-31984 | A denial-of-service vulnerability caused by unbounded resource allocation was discovered in the audit logging functionality, due to a missing size limit on input recorded into audit entries. An unauthenticated attacker can submit requests containing excessively large input that is recorded into audit entries, possibly exhausting the available disk space and rendering the system inoperable. |
| CVE-2026-50328 | Uncaught exception in Windows Server Update Service allows an unauthorized attacker to perform tampering over a network. |
| CVE-2026-57788 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Edge-Themes Aalto aalto allows PHP Local File Inclusion.This issue affects Aalto: from n/a through <= 1.8. |
| CVE-2026-57111 | Permissive Cross-Origin Resource Sharing (CORS) in the REST API (helix-rest, org.apache.helix.rest.server.filters.CORSFilter) in Apache Helix through 2.0.0 on all platforms allows a remote attacker controlling a web page visited by an authorized user to read responses from and issue cross-origin requests to administrative REST endpoints via a cross-origin request from an arbitrary origin, since the filter unconditionally returns Access-Control-Allow-Origin: * together with Access-Control-Allow-Credentials: true and reflects arbitrary Access-Control-Request-Method / Access-Control-Request-Headers values in preflight responses. Users are recommended to upgrade to version 2.0.1, which fixes this issue. |
| CVE-2026-50330 | Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to elevate privileges over a network. |
| CVE-2026-57789 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in jwsthemes Aqua aqua allows PHP Local File Inclusion.This issue affects Aqua: from n/a through <= 5.1.2. |
| CVE-2026-9700 | The Eventer plugin for WordPress is vulnerable to time-based SQL Injection via the ‘code’ parameter in all versions up to, and including, 4.4.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. |
| CVE-2026-57790 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove Billey billey allows PHP Local File Inclusion.This issue affects Billey: from n/a through <= 2.1.8. |
| CVE-2026- | Authorization bypass through User-Controlled key vulnerability in PAVO Financial Technology Solutions Inc. PAVO Pay allows Exploitation of Trusted Identifiers. |

| | |
|---|---|
| 1989 | This issue affects PAVO Pay: through 09072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-57791 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove Brook brook allows PHP Local File Inclusion.This issue affects Brook: from n/a through <= 2.9.0. |
| CVE-2026-15335 | The Booking Package plugin for WordPress is vulnerable to generic SQL Injection via 'email' Form Parameter (form<N>) in all versions up to, and including, 1.7.20 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The vulnerable REST API endpoint /wp-json/booking-package/v1/request is registered with permission_callback: __return_true and wp_magic_quotes does not apply to REST-sourced $_POST values, meaning single quotes in the payload reach the SQL sink intact without any authentication requirement. The impact of this is severely limited as the vulnerable parameter goes through is_email. |
| CVE-2026-57792 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Dør dor allows PHP Local File Inclusion.This issue affects Dør: from n/a through <= 2.4.1. |
| CVE-2026-57793 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Flow flow allows PHP Local File Inclusion.This issue affects Flow: from n/a through <= 1.8. |
| CVE-2026-57794 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in uxper Golo Framework golo-framework allows PHP Local File Inclusion.This issue affects Golo Framework: from n/a through <= 1.7.3. |
| CVE-2026-57795 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in themelexus Kitchor kitchor allows PHP Local File Inclusion.This issue affects Kitchor: from n/a through <= 1.4.3. |
| CVE-2026-0288 | Multiple buffer overflow vulnerabilities in the User-ID Terminal Server Agent (TSA) component of Palo Alto Networks PAN-OS software allow an unauthenticated attacker with network access to cause a denial of service (DoS) condition or potentially execute arbitrary code by sending specially crafted network traffic. The security risk posed by this issue is minimized when the User-ID Terminal Server Agent connectivity is restricted to only trusted internal IP addresses according to our recommended best practice deployment guidelines https://docs.paloaltonetworks.com/ngfw/help/10-2/user-identification/device-user-identification-terminal-services-agents#:~:text=To%20minimize%20security%20risk%2C%20restrict%20TS%20Agent%20connectivity%20to%20trusted%20internal%20IP%20addresses%20only. . Panorama is not impacted by this vulnerability. |
| CVE-2026-56170 | Allocation of resources without limits or throttling in ASP.NET Core allows an unauthorized attacker to deny service over a network. |
| CVE-2026-57796 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in VLThemes Leedo leedo allows PHP Local File Inclusion.This issue affects Leedo: from n/a through <= 3.0.0. |
| CVE-2026-56669 | Elysia is a Typescript framework for request validation, type inference, OpenAPI documentation, and client-server communication. Prior to 1.4.29, Elysia uses getAll in form data normalization for multipart/form-data endpoints, causing the amount of work to grow quadratically with the number of unique key-value pairs and allowing CPU exhaustion. This issue is fixed in version 1.4.29. |
| CVE-2026-11571 | The Everest Forms WordPress plugin before 3.5.0 does not reliably delete temporary CSV files generated during email-notification processing and leaves them publicly accessible in the uploads directory, allowing unauthenticated attackers to retrieve other users' form submission records via predictable, enumerable filenames. |
| CVE-2026-54063 | Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. Prior to 2.11.0, the checkSheet() function in github.com/xuri/excelize/v2 uses an attacker-controlled <row r="N"> XML attribute value directly as the length argument to make([]xlsxRow, row) without validating it against the Excel row limit (TotalRows = 1,048,576). A specially crafted XLSX file can trigger two denial-of-service variants: (A) an out-of-memory process kill when r=2147483647 forces a ~16 GB allocation attempt, and (B) a runtime panic via out-of-bounds slice indexing when r=-1. Any service that opens attacker-supplied XLSX files and calls GetCellValue is affected. No authentication is required. This issue is fixed in version 2.11.0. |
| CVE-2026-59886 | pyasn1 is a generic ASN.1 library for Python. Prior to 0.6.4, the univ.Real type converted its mantissa, base, and exponent value to a Python float using exact big-integer exponentiation. A BER, CER, or DER encoded REAL value only a few bytes long can carry a very large exponent, causing float conversion through prettyPrint(), str(), comparison, arithmetic, int(), or an explicit float() call to consume excessive CPU and memory and hang applications that decode untrusted ASN.1 data and then print, log, or compare decoded objects. This issue is fixed in version 0.6.4. |
| CVE-2026-57729 | Missing Authorization vulnerability in UX-themes Flatsome flatsome allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Flatsome: from n/a through <= 3.20.5. |
| CVE-2026-15111 | Use after free in Views in Google Chrome prior to 150.0.7871.115 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-55470 | HAPI FHIR is a complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. Prior to 6.9.10, the fix for CVE-2026-45367 incompletely patched the DSTU2 module, leaving FHIRPathEngine.matches() in org.hl7.fhir.dstu2/utils/FHIRPathEngine.java to call raw String.matches(sw) without RegexTimeout protection while replaceMatches() was updated, allowing an unauthenticated attacker to trigger catastrophic regex backtracking and exhaust server CPU. This issue is fixed in version 6.9.10. |
| CVE-2026-56303 | Capgo before 12.128.2 contains an information disclosure vulnerability in the find_apikey_by_value PostgreSQL function marked SECURITY DEFINER and executable by the anon role. Unauthenticated attackers can call this function via the /rest/v1/rpc/find_apikey_by_value endpoint to retrieve sensitive API key metadata including user_id, mode, org scoping, and expiration details when supplied a valid key value. |
| CVE-2026-9282 | The W3 Total Cache plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.9.4 via the setupSources function. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. Exploitation requires enabling manual minify mode and supplying a manual-format minify filename so that the hash is empty and the f_array[] entries are not overwritten before reaching setupSources(). |
| CVE- | |

| | |
|---|---|
| 2026-51535 | In OpENer 2.3.0 (commit 76b95cf), a resource exhaustion (Denial of Service) vulnerability exists in its network processing loop. |
| CVE-2026-15117 | Use after free in Payments in Google Chrome prior to 150.0.7871.115 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) |
| CVE-2024-7708 | For requests that have a body, but reading the body may end up in reading 0 bytes, there is a buffer leak. This is particularly the case for 100-Continue, but any request where the network is slow can leak. |
| CVE-2026-44160 | Fluentd collects events from various data sources and writes them to files, RDBMS, NoSQL, IaaS, SaaS, Hadoop and so on. Prior to 1.19.3, Fluentd's in_http and in_forward plugins support gzip-compressed data but enforce limits only on compressed payloads through settings such as body_size_limit and chunk_size_limit, allowing crafted compressed payloads to decompress in memory to an excessive size and cause denial of service through memory exhaustion. This issue is fixed in version 1.19.3. |
| CVE-2026-44025 | Fluentd collects events from various data sources and writes them to files, RDBMS, NoSQL, IaaS, SaaS, Hadoop and so on. Prior to 1.19.3, Fluentd's Monitor Agent plugin in_monitor_agent exposes internal metrics and plugin information via a REST API, and responses from /api/plugins.json and related endpoints unintentionally include internal instance variables that may contain database passwords, API keys, or cloud credentials. This issue is fixed in version 1.19.3. |
| CVE-2026-57727 | Missing Authorization vulnerability in Themeum Kirki kirki allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Kirki: from n/a through <= 6.0.13. |
| CVE-2026-10051 | In Eclipse Jetty, a first HTTP/1.1 request with trailers causes the server to retain the trailers in subsequent requests performed over the same connection. Subsequent request that do not have trailers report the trailers of the first request. Subsequent request that do have trailers report the union of trailers of the first request and the current request. |
| CVE-2026-31309 | Improper authorization in the /tequilapi/config/user endpoint of Mysterium Node from v1.21.1-rc0 before v1.36.0 allows an unauthenticated attacker to arbitrarily overwrite the node's configuration and achieve a full node takeover via a crafted POST request. |
| CVE-2026-61439 | PraisonAI versions before 4.6.78 contain a prompt injection defense misconfiguration where the block threshold defaults to CRITICAL severity, allowing HIGH-level threats to pass through unblocked. Attackers can submit single-vector prompt injection attacks such as instruction overrides or financial manipulation that trigger HIGH severity detection but are logged without blocking, enabling system prompt extraction and unauthorized tool invocations. |
| CVE-2026-33382 | Several Grafana API endpoints, some of them unauthenticated, do not limit the size of the request body before processing it. An attacker can send very large payloads that force excessive memory allocation, potentially exhausting memory and causing a denial of service. |
| CVE-2026-15075 | In Eclipse Vert.x versions up to and including 4.5.29 (4.x branch) and 5.1.4 (5.x branch), DefaultRedirectHandler (vertx-core) propagates all request headers as-is across cross-origin HTTP 30x redirects. Only Content-Length is stripped; no origin comparison (scheme, host, port) is performed before copying headers to the redirect target. As a result, credential headers, including Authorization, Cookie, Proxy-Authorization, and arbitrary custom headers such as X-API-Token, are forwarded to the redirect destination without the caller's knowledge. An attacker who can cause a Vert.x HttpClient to issue a request that is redirected to an attacker-controlled host (for example, by supplying a URL to a webhook dispatcher, image proxy, or microservice URL fetcher) can capture bearer tokens, basic-auth credentials, session cookies, and API keys attached to the original request. |
| CVE-2026-59885 | pyasn1 is a generic ASN.1 library for Python. Prior to 0.6.4, the BER, CER, and DER decoders process OBJECT IDENTIFIER and RELATIVE-OID values in quadratic time relative to the number of arcs, so a small crafted payload containing an OID with many arcs consumes excessive CPU per decode() call and can deny service to applications that decode untrusted ASN.1 data. The corresponding encoders have the same quadratic behavior when an application re-encodes previously decoded attacker-supplied values. This issue is fixed in version 0.6.4. |
| CVE-2026-59884 | pyasn1 is a generic ASN.1 library for Python. Prior to 0.6.4, the BER decoder shared by the CER and DER codecs parses long-form tags by accumulating continuation octets without an upper bound on the tag ID size, allowing a crafted input to force construction of an arbitrarily large integer with CPU cost growing quadratically and to trigger unhandled ValueError exceptions in Python 3.11+ error formatting paths. Any application decoding untrusted BER, CER, or DER input is affected. This issue is fixed in version 0.6.4. |
| CVE-2026-54499 | Stanza is a Stanford NLP Python library for tokenization, sentence segmentation, NER, and parsing of many human languages. Prior to 1.12.2, Stanza model loaders such as stanza.models.common.pretrain.Pretrain.load() attempt torch.load(..., weights_only=True) but fall back to torch.load(..., weights_only=False) on attacker-controllable pickle.UnpicklingError, allowing a malicious .pt pretrain or model file to execute arbitrary pickle code when a Stanza NLP pipeline loads it. This issue is fixed in version 1.12.2. |
| CVE-2026-54772 | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, an unauthenticated remote attacker that can reach a NetTcpBinding, NetNamedPipeBinding, or UnixDomainSocketBinding endpoint can trigger premature EOF handling in the CoreWCF net.tcp, net.pipe, or net.uds framing handshake and pin one server thread-pool worker at full CPU per connection. This issue is fixed in versions 1.8.1 and 1.9.1. |
| CVE-2026-59200 | Pillow is a Python imaging library. From 5.1.0 until 12.3.0, PdfParser.PdfStream.decode() in PIL/PdfParser.py calls zlib.decompress() with bufsize set to the PDF stream Length field without bounding the decompressed output size, allowing a crafted FlateDecode PDF stream to exhaust memory from a small file. This issue is fixed in version 12.3.0. |
| CVE-2025-70796 | An unauthenticated path traversal vulnerability exists in the web management interface of WTI (Wireless Technology, Inc.) version 3.5.0.r 2024/05/24 00:00:00. An unauthenticated attacker can craft malicious HTTP requests containing traversal sequences to access files outside of the intended web root directory. This may allow disclosure of sensitive system files and configuration data |
| CVE-2026-15076 | In versions up to and including 4.5.29 (4.x branch) and 5.1.4 (5.x branch), the WebClientSession component of Eclipse Vert.x Web Client does not validate that the Domain attribute of a Set-Cookie response header matches the originating server's domain, in violation of RFC 6265 section 5.3. An attacker who controls any server that the victim application contacts can inject a cookie scoped to an arbitrary third-party domain; because the session store performs no cross-domain ownership check, it stores and later transmits that cookie to the targeted domain. When the victim application subsequently sends a request to the targeted domain using the same WebClientSession, it presents the attacker-injected cookie, causing the receiving service to process the request under the attacker's account. Sensitive data included in the victim application's requests, such as payment amounts, card details, or other API payloads, may then be accessible to the attacker through their own account on that service. |
| CVE-2026-4661 | The WP CTA – Sticky CTA Builder, Generate Leads, Promote Sales plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'fildname' parameter in all versions up to, and including, 2.2.2. This is due to insufficient escaping of user-supplied column names in the ajaxCheck() method and lack of preparation in the $wpdb->update() call. The vulnerability is compounded by the complete absence of authorization checks and the endpoint being registered for unauthenticated users via wp_ajax_nopriv_. This makes it possible for unauthenticated attackers to inject arbitrary SQL queries and extract sensitive information from the database via time-based blind SQL injection techniques, including administrator password hashes. |

| | |
|---|---|
| CVE-2026-39244 | adm-zip before 0.5.18 is vulnerable to denial of service via a crafted ZIP file with a manipulated uncompressed size header field. In zipEntry.js line 103, Buffer.alloc(_centralHeader.size) allocates memory based on the declared uncompressed size from the ZIP central directory header without validating it against the actual compressed data size or imposing any upper bound. The size value is read directly from the binary header at entryHeader.js line 266 with no bounds check. An attacker can craft a ~120-byte ZIP file that declares ~4GB uncompressed size, causing a memory allocation amplification ratio of over 33 million to 1. The allocation occurs before CRC validation, so the malicious payload cannot be rejected early. All extraction and read methods are affected: readFile(), readAsText(), extractEntryTo(), extractAllTo(), extractAllToAsync(), test(), and entry.getData(). Any application accepting untrusted ZIP files via adm-zip is vulnerable to immediate process crash. |
| CVE-2026-57378 | Missing Authorization vulnerability in Phil Kurth Advanced Forms advanced-forms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Advanced Forms: from n/a through <= 1.9.3.7. |
| CVE-2026-50696 | Heap-based buffer overflow in Windows Internet Key Exchange (IKE) Protocol allows an unauthorized attacker to deny service over a network. |
| CVE-2026-57798 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in SaurabhSharma NewsPlus Shortcodes newsplus-shortcodes allows PHP Local File Inclusion.This issue affects NewsPlus Shortcodes: from n/a through <= 4.2.0. |
| CVE-2026-57799 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in uxper Nuss nuss allows PHP Local File Inclusion.This issue affects Nuss: from n/a through <= 1.3.6. |
| CVE-2026-51604 | A stack-based buffer overflow vulnerability in the RTSP service of Tenda CP3 V3.0 (firmware V31.1.9.91) allows an unauthenticated remote attacker to cause a denial of service via a crafted PLAY request. |
| CVE-2026-59692 | A stack buffer overflow vulnerability was found in GStreamer's DTLS plugin. During a DTLS handshake, the peer certificate Subject Distinguished Name is printed into a fixed-size 2048-byte stack buffer without bounds checking. A remote unauthenticated attacker can send a certificate with an oversized Subject DN that exceeds the buffer, causing a stack buffer overflow and process crash, resulting in denial of service. |
| CVE-2026-57815 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WPMU DEV - Your All-in-One WordPress Platform Forminator forminator allows Path Traversal.This issue affects Forminator: from n/a through <= 1.55.0.2. |
| CVE-2026-12707 | Summary Cloudflare quiche was discovered to be vulnerable to memory resource exhaustion due to unbounded queuing of post-handshake client migration events. Impact quiche supports the connection migration features described in Section 9 of RFC 9000, which allows a single QUIC connection to survive changes in the network path. Although quiche implements the protections described in Section 9.3 of RFC 9000 to limit server state commitment, it was discovered that the collection of PathEvents, intended to be consumed by applications via the path_event_next() function, was not bounded. Once the QUIC handshake completed, a peer could exploit rapid source address migration in order to cause unbounded queuing of the PathEvent::ReusedSourceConnectionId type. Servers are vulnerable even if active connection migration is disabled. Mitigation: * Applications can call path_event_next() to drain the PathEvent collection, mitigating the attack. * Users are requested to upgrade to quiche 0.29.3 which is the earliest version that prevents excessive queueing of PathEvent::ReusedSourceConnectionId. |
| CVE-2026-13462 | PayRange Android app, version 7.0.7 and below, contains an SSL bypass vulnerability that allows invalid certificates to be accepted in application webviews. A remote and unauthenticated attacker can steal information that the user sends. |
| CVE-2026-55404 | yt-dlp and youtube-dl are command-line audio/video downloaders. Prior to 2026.7.4, the --write-link, --write-url-link, and --write-desktop-link options can write .url or .desktop shortcut files using attacker-controlled webpage_url or filename metadata without sufficient validation or escaping, allowing malicious file:// URI injection on Windows or newline-based desktop entry key injection on Linux that can execute commands if the generated shortcut is opened. This issue is fixed in version 2026.7.4. |
| CVE-2026-56250 | Capgo before 12.128.2 allows upload-scoped API keys to modify the mutable app_versions.r2_path field through PostgREST, enabling retargeting to arbitrary R2 bundle objects. Attackers can patch r2_path to point to victim objects, soft-delete the attacker-controlled version, and trigger the on_version_update cleanup function to delete the victim R2 object, causing denial of service and bundle availability disruption. |
| CVE-2026-15308 | The incremental HTML parser (html.parser.HTMLParser) allows for CPU denial-of-service through repeated unterminated markup declarations when processing uncontrolled data. |
| CVE-2026-58101 | Crypt::OpenSSL::X509 versions before 2.1.3 for Perl allow denial of service via NULL pointer dereference. X509V3_EXT_d2i(ext) returns NULL when an extension's DER value fails to parse. basicC, ia5string, and auth_att dereference its result without a NULL check. keyid_data also dereferences akid->keyid, which is NULL for an empty AKI SEQUENCE (DER 30 00) even when the parse succeeds. A caller invoking an affected helper on an extension from an untrusted certificate triggers a SIGSEGV that crashes the Perl process. |
| CVE-2026-51600 | Tenda CP3 V3.0 firmware V31.1.9.91 does not validate the Content-Length header field in RTSP requests (including DESCRIBE, SETUP, and PLAY methods). When a request carrying a Content-Length header is received without a corresponding message body, the RTSP parser enters a persistent body-awaiting state, causing the affected TCP connection to become permanently non-functional. The device does not actively close the connection, resulting in a TCP resource leak. This issue can be exploited by an unauthenticated remote attacker to cause a denial-of-service condition. |
| CVE-2026-51601 | Tenda CP3 V3.0 firmware V31.1.9.91 contains a stack-based buffer overflow in the RTSP service. The device fails to validate the length of the clock= value in the Range header field when processing a PLAY request. An unauthenticated remote attacker who has completed a standard RTSP session handshake can send a PLAY request with an excessively long clock= value to cause the RTSP service to crash. |
| CVE-2026-51602 | A stack-based buffer overflow vulnerability in the RTSP service of Tenda CP3 V3.0 (firmware V31.1.9.91) allows an unauthenticated remote attacker to cause a denial of service via a crafted SETUP request. The RTSP service's second-stage URL routing parser fails to validate the length of the URL field in the first SETUP request. By supplying a URL consisting of exactly four consecutive repetitions of a valid RTSP URL, an attacker can bypass first-stage format validation and trigger a stack buffer overflow, causing an immediate crash of the RTSP service process and rendering the device inaccessible to all clients on the local network. |
| CVE-2026-51603 | A stack-based buffer overflow vulnerability in the RTSP service of Tenda CP3 V3.0 (firmware V31.1.9.91) allows an unauthenticated remote attacker to cause a denial of service via a crafted second SETUP request. After completing the OPTIONS, DESCRIBE, and a legitimate first SETUP request to obtain a valid session ID, the RTSP service's second-stage URL routing parser fails to validate the length of the URL field in the subsequent SETUP request. By supplying a URL consisting of exactly four consecutive repetitions of a valid RTSP URL, an attacker can bypass first-stage format validation and trigger a stack buffer overflow, causing an immediate crash of the RTSP service process and rendering the device inaccessible to all clients on the local network. |
| CVE- | A stack-based buffer overflow vulnerability in the RTSP service of Tenda CP3 V3.0 (firmware V31.1.9.991) allows an unauthenticated remote attacker to cause a |

| | |
|---|---|
| 2026-51605 | denial of service via a crafted TEARDOWN request. |
| CVE-2026-54983 | Stack-based buffer overflow in Active Directory Federation Services (AD FS) allows an unauthorized attacker to deny service over a network. |
| CVE-2026-51606 | An improper input handling vulnerability in the RTSP service of Tenda CP3 V3.0 (firmware V31.1.9.91) causes the device to abruptly terminate the TCP connection with a RST packet when a request containing an oversized field value is received, without returning any RFC 2326-compliant error response. This behavior affects the request-line URL field and header field values across multiple RTSP request types. |
| CVE-2026-15584 | A privilege escalation vulnerability was found in the incluster-checks tool for OpenShift. The tool creates privileged debug pods with host filesystem access in the shared default namespace, where any user with the standard edit role can exec into them and obtain root access on cluster nodes. |
| CVE-2026-40467 | Use After Free vulnerability has been found in "io.c" program file of gawk (do_getline_redir() routine). This issue may lead to a crash. It affects gawk in versions 5.4.0 and below. |
| CVE-2026-54119 | Loop with unreachable exit condition ('infinite loop') in Windows Active Directory allows an unauthorized attacker to deny service over a network. |
| CVE-2026-62328 | 9Router through version 0.4.41 contain an unauthenticated information disclosure vulnerability that allows remote attackers to access sensitive user data by sending requests to unprotected API endpoints. Attackers can enumerate paginated request logs and retrieve complete AI conversation histories including system prompts, user messages, assistant responses, tool calls, and user email addresses by querying the request-logs and request-details API routes which lack authentication middleware. |
| CVE-2026-59199 | Pillow is a Python imaging library. Prior to 12.3.0, Pillow public image coordinate APIs can trigger a native heap out-of-bounds write when given coordinates near the signed 32-bit integer limits in Image.paste(), Image.crop(), or Image.alpha_composite(). This issue is fixed in version 12.3.0. |
| CVE-2026-40553 | Buffer overflow vulnerability has been found in "extension/readdir.c" program file of gawk (ftype() routine). This issue could be used to crash the program and potentially to achieve code execution, although the latter has not been confirmed to be feasible. It affects gawk in versions 5.4.0 and below. |
| CVE-2026-59937 | pypdf is a free and open-source pure-python PDF library. Prior to 6.14.0, an attacker can craft a PDF with repeated malformed cross-reference streams that cause pypdf to spend long runtimes recovering broken cross-reference table entries. This issue is fixed in version 6.14.0. |
| CVE-2026-56238 | Capgo before 12.128.2 contains an information disclosure vulnerability in the Supabase PostgREST global_stats endpoint that allows unauthenticated attackers to read sensitive financial and operational metrics using only the public apikey. Remote attackers can query the /rest/v1/global_stats endpoint to expose MRR, total revenue, plan-tier revenue breakdown, customer counts, and operational telemetry. |
| CVE-2026-59204 | Pillow is a Python imaging library. From 8.2.0 through 12.2.0, src/libImaging/Jpeg2KDecode.c accumulates total_component_width across every tile in a JPEG2000 image instead of recomputing it per tile, allowing a crafted tiled JPEG2000 file to force substantially higher transient memory usage and trigger out-of-memory failures during decoding. This issue is fixed in version 12.3.0. |
| CVE-2026-59928 | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, a Markdown document containing many repeated or distinct reference-link definitions causes quadratic work in src/mistune/block_parser.py and the ref_links environment dictionary handling, allowing denial of service through CPU exhaustion. This issue is fixed in version 3.3.0. |
| CVE-2026-59925 | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, long sequences of well-formed double-asterisk or triple-asterisk emphasis pairs around a character cause quadratic work in src/mistune/inline_parser.py because the parser scans forward for matching close markers from every potential opening run, allowing denial of service in default Mistune parsing. This issue is fixed in version 3.3.0. |
| CVE-2026-50355 | Stack-based buffer overflow in Active Directory Federation Services allows an unauthorized attacker to deny service over a network. |
| CVE-2026-12523 | Summary Cloudflare quiche's HTTP/3 layer was discovered to be vulnerable to resource exhaustion (i.e., memory) by means of specially crafted HTTP/3 frames. Impact HTTP/3 defines multiple frame types to support HTTP message exchanges and connection management. Each frame has a length and a payload whose length depends on the frame type. quiche was found to be vulnerable when parsing some frame types to pre-allocating memory based on the declared length. An attacker would not need to send the number of declared bytes to trigger this issue. In addition, quiche was found to not apply QPACK decompression limits correctly. This could allow an attacker to send specially crafted HEADERS frames that would cause more memory commitment than otherwise advertised by MAX_FIELD_SECTION_SIZE (configured by set_max_field_section_size()). Mitigation: * Users are requested to upgrade to quiche 0.29.3 which is the earliest version containing the fix for this issue. Credits: Disclosed responsibly by Sébastien Féry |
| CVE-2026-56292 | A SQLi vulnerability in AcyMailing component < 10.11.1 for Joomla was discovered. Exploiting this flaw can lead to unauthorized database access and data leakage. |
| CVE-2026-55760 | Handlebars.java provides logic-less and semantic Mustache templates with Java. Prior to 4.5.2, applications that pass user-controlled input to Handlebars.compile() using FileTemplateLoader or ClassPathTemplateLoader are vulnerable to path traversal, allowing arbitrary file read through template names derived from URL path parameters, request parameters, or other user-controlled sources. This issue is fixed in version 4.5.2. |
| CVE-2026-51105 | Buffer Overflow vulnerability in aMULE-Project aMule v.2.3.3 allows a remote attacker to cause a denial of service via the OP_SERVERMESSAGE Handler. |
| CVE-2026-57800 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Edge-Themes Overworld overworld allows PHP Local File Inclusion.This issue affects Overworld: from n/a through <= 1.5. |
| CVE-2026-57705 | Missing Authorization vulnerability in Nexcess Event Tickets event-tickets allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Event Tickets: from n/a through <= 5.28.5. |
| CVE- | httplib2 is a comprehensive HTTP client library for Python. Prior to 0.32.0, httplib2 performs unbounded decompression of HTTP response bodies encoded with |

| | |
|---|---|
| 2026-59939 | Content-Encoding: gzip or deflate in _decompressContent in httplib2/init.py, allowing a malicious or compromised HTTP server to return a small compressed payload that expands to an arbitrarily large size in memory and causes MemoryError or OOM-kill in the client process. This issue is fixed in version 0.32.0. |
| CVE-2026-59936 | pypdf is a free and open-source pure-python PDF library. Prior to 6.14.1, an attacker can craft a PDF with a page content stream containing a not terminated inline image, causing an infinite loop during inline image end marker detection such as when extracting page text. This issue is fixed in version 6.14.1. |
| CVE-2026-59935 | pypdf is a free and open-source pure-python PDF library. Prior to 6.14.2, an attacker can craft a PDF with a page content stream containing a not terminated inline image that uses the ASCII85 or ASCIIHex filters, causing an infinite loop during parsing such as when extracting page text. This issue is fixed in version 6.14.2. |
| CVE-2026-57697 | Authentication Bypass Using an Alternate Path or Channel vulnerability in Metagauss ProfileGrid profilegrid-user-profiles-groups-and-communities allows Password Recovery Exploitation.This issue affects ProfileGrid : from n/a through <= 5.9.9.6. |
| CVE-2026-55175 | Spinnaker is an open source, multi-cloud continuous delivery platform. Prior to versions 2026.1.1, 2026.0.3, 2025.4.4, and 2025.3.4 on their respective release lines, Kustomize bake operations allow unsafe YAML tag processing in rosco manifests. This can lead to remote code execution on rosco pods when performing Kustomize bakes. This issue is fixed in versions 2026.1.1, 2026.0.3, 2025.4.4, and 2025.3.4. |
| CVE-2026-44383 | Multiple connections to the backend using the same charging station ID are allowed, which could allow an attacker to deploy multiple instances of malicious OCPP clients to overwhelm the backend. |
| CVE-2026-42952 | Previously, there was no throttling on repeated authentication attempts to the charging station backend, which could allow an attacker to execute a denial-of-service attack. |
| CVE-2026-57801 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes SetSail setsail allows PHP Local File Inclusion.This issue affects SetSail: from n/a through <= 2.1. |
| CVE-2026-57802 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Struktur struktur allows PHP Local File Inclusion.This issue affects Struktur: from n/a through <= 2.5.1. |
| CVE-2026-59803 | rpcx through 1.9.3, fixed in commit 047aec1, contains a denial-of-service vulnerability in protocol.Message.Decode (protocol/message.go). When a message has the compression flag set, the payload is gzip-decompressed via util.Unzip with no limit on the decompressed output size. The only built-in size guard, protocol.MaxMessageLength, is checked against the compressed on-the-wire frame length, not the decompressed size, so it provides no protection. Because decoding (and decompression) occurs in readRequest before authentication, a single unauthenticated connection can send a small (under 2 MB) gzip-compressed message that expands to gigabytes of heap allocation, leading to out-of-memory conditions and service unavailability. |
| CVE-2026-56226 | Capgo (Cap-go/capgo) before 12.128.2 exposes the Supabase PostgREST RPC function public.get_orgs_v6(userid uuid), which is SECURITY DEFINER and granted to the anon role, allowing unauthenticated access. Because the function accepts a caller-supplied user UUID without verifying it matches the authenticated user, an attacker using only the public publishable API key can query POST /rest/v1/rpc/get_orgs_v6 with an arbitrary user UUID to retrieve that user's organization membership, roles, subscription/trial metadata, and management_email (PII). |
| CVE-2026-57803 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Struktur Core struktur-core allows PHP Local File Inclusion.This issue affects Struktur Core: from n/a through <= 2.5.1. |
| CVE-2026-60108 | Zeek before 8.0.9 contains an uncontrolled memory consumption vulnerability in the FTP analyzer that allows unauthenticated remote attackers to cause process termination by sending a crafted FTP control session negotiating AUTH GSSAPI followed by a large ADAT control line. Attackers can exploit the NVT_Analyzer component's lack of a maximum line length check, causing it to continuously double its internal buffer without bounds during base64 decoding of an attacker-controlled ADAT token, resulting in denial of service of the Zeek sensor. |
| CVE-2026-60109 | Zeek before 8.0.9 contains a null pointer dereference vulnerability in its Kerberos protocol analyzer that allows unauthenticated remote attackers to crash the sensor by sending a crafted KRB_ERROR message with error-code 25 (KDC_ERR_PREAUTH_REQUIRED) containing a PA-DATA element with padata-type 2, 3, 11, or 19. Attackers can exploit a parser and analyzer state mismatch where proc_padata() dereferences an uninitialized pa_data_element field selected by the wrong parsing arm, triggering a crash via a single UDP or TCP packet to port 88 without any credentials or prior authentication. |
| CVE-2026-58250 | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.12.8 and 2.11.17, an unauthenticated peer with network access to a leafnode listener with compression enabled could crash the server during the pre-authentication leafnode handshake by sending repeated leafnode INFO protocol messages before authentication and account setup completed. This issue is fixed in versions 2.12.8 and 2.11.17. |
| CVE-2026-60114 | Sustainable Irrigation Platform (SIP) through version 5.2.16 contains a path traversal vulnerability that allows attackers with access to the restore functionality to write files to arbitrary locations by uploading crafted JSON backup files with unvalidated keys used to construct file paths. Attackers can exploit the lack of key validation in the JSON restore process, combined with the absence of a required passphrase in the default configuration or the default passphrase 'opendoor', to write arbitrary JSON files outside the intended data directory. |
| CVE-2026-11404 | Cesanta Mongoose before 7.22 contains an out-of-bounds read in the built-in TLS server function mg_tls_server_recv_hello(), which uses an attacker-controlled session_id_len byte from a TLS ClientHello as a buffer index without validating it against the length of received data. A remote, unauthenticated attacker can send a single crafted ClientHello with an oversized session id length to read past the receive buffer, crashing any HTTPS, MQTTS, or WSS service built on MG_TLS_BUILTIN. |
| CVE-2025-53379 | A out-of-bounds read vulnerability in Fortinet FortiAuthenticator 6.6.0 through 6.6.2, FortiAuthenticator 6.5 all versions may allow a remote unauthenticated attacker to retrieve sensitive information via a specially crafted request. |
| CVE-2026-57804 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CodexThemes TheGem Theme Elements (for Elementor) thegem-elements-elementor allows PHP Local File Inclusion.This issue affects TheGem Theme Elements (for Elementor): from n/a through <= 5.11.1. |
| CVE-2026-57805 | Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Tonda tonda allows PHP Local File Inclusion.This issue affects Tonda: from n/a through <= 2.5. |
| CVE-2026- | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.3 and 2.12.12, an unauthenticated MQTT client could cause the server to retain large incomplete MQTT CONNECT packets before authentication completed, consuming server memory while the parser waited for |

| | |
|---|---|
| 58210 | the advertised MQTT packet length. This issue is fixed in versions 2.14.3 and 2.12.12. |
| CVE-2026-53450 | Coturn is a free open source implementation of TURN and STUN Server. Prior to 4.13.0, coturn rejects loopback peers by default unless allow-loopback-peers is enabled, but the default loopback guard can be bypassed by using the IPv4-mapped IPv6 peer address ::ffff:127.0.0.1 in a TURN XOR-PEER-ADDRESS attribute. ioa_addr_is_loopback checks for the literal IPv6 loopback shape before IPv4-mapped IPv6 handling, so good_peer_addr does not apply the default loopback rejection and an authenticated TURN client can expose services bound only to localhost on the coturn host through TURN relay traffic. This issue is fixed in version 4.13.0. |
| CVE-2026-54919 | cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. In affected Mbed TLS backend versions from 0.31.0 through 0.46.1 and wolfSSL backend versions from 0.33.0 through 0.46.1, when cpp-httplib is built with CPPHTTPLIB_MBEDTLS_SUPPORT or CPPHTTPLIB_WOLFSSL_SUPPORT and a client connects to an IP-literal host with server certificate verification enabled, SSLClient and Client in HTTPS mode skip certificate chain validation and WebSocketClient on the Mbed TLS backend skips verification altogether, allowing a man-in-the-middle attacker positioned to intercept traffic to present a crafted certificate and read or modify the traffic. This issue is fixed in version 0.47.0. |
| CVE-2026-55672 | ZITADEL is an open source identity management platform. Prior to 3.4.12 and 4.15.2, ZITADEL's OAuth2 and OIDC CodeExchange, RefreshToken, and device token flows fail to verify that the requesting client matches the client that initiated the authorization flow, allowing intercepted grants or refresh tokens to be exchanged under a different client. This issue is fixed in versions 3.4.12 and 4.15.2. |
| CVE-2026-55436 | Coder allows organizations to provision remote development environments via Terraform. Starting in version 2.30.0 and prior to versions 2.32.7, 2.33.8, and 2.34.2, the AI Bridge Proxy (`aibridgeproxyd`) created a goproxy server whose default transport set `InsecureSkipVerify: true` and only assigned a secure transport when an upstream proxy was configured. In the default configuration (no upstream proxy), outbound HTTPS to the Coder access URL accepted any TLS certificate. Practical exploitation requires an on-path (man-in-the-middle) position between the AI Bridge Proxy and the Coder server. Deployments where they are co-located over loopback are effectively unaffected. The fix in versions 2.32.7, 2.33.8, and 2.34.2 applies the secure transport (TLS 1.2 or higher using system root CAs) unconditionally. As a workaround, ensure the Coder access URL uses a trusted certificate and secure the network path between the AI Bridge Proxy and the Coder server (for example, loopback or mTLS). |
| CVE-2026-54429 | A vulnerability has been identified in SIMATIC S7-PLCSIM Advanced (All versions). Affected devices do not properly handle high-volume multicast network traffic, which can exhaust available memory resources in the affected application. This could allow an unauthenticated attacker on the local network segment to cause a denial-of-service condition of the affected application. The affected application becomes inaccessible and requires a manual restart; no project data is lost. Successful exploitation requires a specific project configuration to be already active on the targeted instance. |
| CVE-2026-62240 | CrewAI before 1.15.1 contains a server-side request forgery vulnerability in the validate_url function that performs one-shot DNS resolution and blocklist checks before returning the original URL unchanged. Attackers can bypass the security filter by supplying URLs that redirect to internal addresses or use DNS rebinding techniques to access internal services and cloud metadata endpoints. |
| CVE-2026-56676 | 9Router is an AI router & token saver. Prior to 0.5.2, 9router validates image URLs by resolving the host before fetching, but open-sse/translator/concerns/image.js performs the later server-side image fetch with a separate DNS resolution. An authenticated attacker with access to the LLM proxy can use a vision-capable model and an attacker-controlled DNS name that first resolves to a public IP and then rebinds to an internal address, allowing server-side requests to internal-only HTTP services. This issue is fixed in version 0.5.2. |
| CVE-2026-54127 | Use after free in Windows Hyper-V allows an unauthorized attacker to elevate privileges locally. |
| CVE-2026-54774 | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, SamlSerializer skips final SignatureValue verification when a CoreWCF service validates SAML tokens using a non-X.509 signing token, allowing an attacker to reference a non-X.509 SecurityToken key identifier and bypass assertion signature verification. This issue is fixed in versions 1.8.1 and 1.9.1. |
| CVE-2026-54783 | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, CoreWCF WS-Security endorsing and supporting signature verification does not ensure the selected ds:Signature covers the expected Security header target, allowing an attacker with one captured signed SOAP envelope to replay arbitrary service operations as the victim principal. This issue is fixed in versions 1.8.1 and 1.9.1. |
| CVE-2026-49969 | Laravel-Mediable before 7.0.0 contains a server-side request forgery vulnerability that allows remote attackers to issue arbitrary HTTP requests from the server by supplying unvalidated caller-controlled URLs to endpoints backed by MediaUploader::fromSource(). Attackers can craft URLs targeting RFC-1918 addresses, loopback interfaces, cloud metadata endpoints, or file:// URIs through RemoteUrlAdapter to reach internal infrastructure, retrieve sensitive files, and exfiltrate cloud credentials such as IAM tokens from instance metadata services. |
| CVE-2026-15081 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Drupal Location Selector allows SQL Injection. This issue affects Location Selector versions: from 0.0.0 to 1.3.0. |
| CVE-2026-10665 | In Zephyr's WireGuard subsystem (subsys/net/lib/wireguard), wg_process_data_message() in wg_crypto.c linearizes an inbound transport-data payload into a fixed pool buffer of CONFIG_WIREGUARD_BUF_LEN bytes before decryption. The call net_buf_linearize(buf->data, data_len, pkt->buffer, ..., data_len) passed the attacker-derived data_len as both the destination capacity and the copy length, defeating the function's internal len = min(len, dst_len) bound. data_len is derived from the received UDP datagram length and is only lower-bounded by wg_ctrl_recv() (no upper bound). When data_len exceeds CONFIG_WIREGUARD_BUF_LEN — e.g. when the buffer length is lowered below the link MTU, on links with MTU above the buffer size, or via reassembled IPv4/IPv6 fragments that exceed it — the underlying memcpy writes past the end of the pool buffer, an out-of-bounds write (CWE-787). The overflow occurs before the Poly1305 authentication check, so it requires only a valid receiver session index rather than a valid authenticator, and is reachable by a malicious or compromised peer (or an on-path attacker driving an established session) over the network, yielding remote memory corruption and at minimum a reliable denial of service. The defect was present in the WireGuard implementation shipped in Zephyr 4.4.0. The fix adds an explicit data_len > CONFIG_WIREGUARD_BUF_LEN rejection and corrects the linearize call to pass net_buf_max_len(buf) as the destination capacity. |
| CVE-2026-54781 | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, CoreWCF SAML token validation does not enforce SubjectConfirmation method URIs or holder-of-key proof keys in SamlSecurityTokenHandler, allowing holder-of-key downgrade or custom confirmation method assertions to authenticate a subject without proving authority over the assertion. This issue is fixed in versions 1.8.1 and 1.9.1. |
| CVE-2026-4017 | Buffer Overflow in the entry handler of the TraceEvent() system call could allow an attacker with local access to cause information disclosure, data tampering or a crash of the QNX Neutrino kernel. |
| CVE-2026-59806 | Gradio before 6.20.0 contains an open redirect and server-side request forgery vulnerability that allows attackers to redirect users to arbitrary URLs or perform client-side SSRF by supplying unvalidated HTTP/HTTPS URLs to the file_fetch() function in the /gradio_api/file= endpoint. Attackers can craft a malicious FileData response targeting internal endpoints such as cloud metadata services to retrieve sensitive credentials including EC2 IAM role credentials. |
| CVE-2026-54784 | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. In version 1.9.0, CoreWCF SPNEGO SecurityContextToken negotiation can expose the proof key recovered from the RSTR when TransportWithMessageCredential with Windows client credentials and session establishment are used, allowing an observer to impersonate the authenticated Windows principal and decrypt or forge WS-SecureConversation traffic. This issue is fixed in |

| | |
|---|---|
| | version 1.9.1. |
| CVE-2026-56776 | n8n before 1.123.55, 2.25.7, and 2.26.2 contains an authorization bypass in the POST /workflows/{workflowId}/test-runs/new endpoint, which authorizes access using the workflow:read scope instead of workflow:execute. An authenticated user with read-only access to a workflow can trigger a real evaluation test run, causing the workflow to execute via the internal workflow runner and resulting in unintended outbound API calls, data mutations, or other side effects in connected downstream systems. The issue primarily affects instances using the Evaluations feature where RBAC project roles grant workflow:read without workflow:execute. |
| CVE-2026-15489 | A vulnerability was identified in RafyMrX TOKO-ONLINE-ROTI up to ddfe1cd587be0a0b5135d8b6e85cce2ec3aece99. Affected by this vulnerability is an unknown functionality of the file proses/login.php. The manipulation of the argument Username leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15517 | A flaw has been found in Jinher OA 1.0. The affected element is an unknown function of the file /C6/JHSoft.Web.PlanSummarize/PlanGiveOut.aspx. This manipulation of the argument httpOID causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-58640 | Heap-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally. |
| CVE-2026-15514 | A weakness has been identified in Metasoft 美特软件 MetaCRM up to 6.4.0 Beta06. This vulnerability affects the function RPCService.query of the file /customizemt/xkq/rpc.jsp of the component PHPRPC Remote Call Interface. Executing a manipulation of the argument phprpc_args can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15703 | A vulnerability was detected in SourceCodester Simple and Nice Shopping Cart Script 1.0. This vulnerability affects unknown code of the file /admin/userproductdeletequery.php. Performing a manipulation of the argument user_id results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used. |
| CVE-2026-15677 | A weakness has been identified in code-projects Online Job Portal 1.0. This affects an unknown function of the file /JobSeekerInsert.php. Executing a manipulation of the argument txtFile can lead to unrestricted upload. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. |
| CVE-2026-15135 | A security flaw has been discovered in code-projects Online Food Order System 1.0. This affects an unknown part of the file /edit_food_items.php. The manipulation of the argument update results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. |
| CVE-2026-15319 | A security vulnerability has been detected in Sipeed PicoClaw up to 0.2.9. This affects the function IPAllowlist of the file web/backend/middleware/access_control.go of the component Launcher. Such manipulation leads to improper access controls. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The name of the patch is 3126. A patch should be applied to remediate this issue. |
| CVE-2026-15676 | A security flaw has been discovered in code-projects Online Job Portal up to 1.0. The impacted element is an unknown function of the file /Admin/DeleteUser.php. Performing a manipulation results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. |
| CVE-2026-50364 | Improper link resolution before file access ('link following') in Windows Server Backup allows an authorized attacker to elevate privileges locally. |
| CVE-2026-15557 | A weakness has been identified in waooAI waoowaoo up to 0.4.1. Affected by this vulnerability is the function getInternalTaskSession/getAuthSession/requireUserAuth/requireProjectAuth/requireProjectAuthLight in the library src/lib/api-auth.ts of the component Internal Task Header Handler. This manipulation of the argument x-internal-user-id request causes improper authentication. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-15137 | A weakness has been identified in code-projects Interview Management System 1.0. This vulnerability affects unknown code of the file \inc\classes\View.php. This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. |
| CVE-2025-45869 | LogicalDOC Enterprise Version up to and before v9.1.1 is vulnerable to Server-Side Request Forgery (SSRF). An unauthenticated attacker can exploit the ShareFileCallback servlet by manipulating input parameters to trigger a server-side request to an attacker-controlled host. |
| CVE-2026-15190 | A vulnerability was detected in SourceCodester Simple and Nice Shopping Cart Script 1.0. This affects an unknown part of the file /login.php. Performing a manipulation of the argument Username results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used. |
| CVE-2026-56667 | ZITADEL is an open source identity management platform. Prior to 4.15.3, ZITADEL Login V2 OIDC and SAML FailedPrecondition error paths return loginSettings.defaultRedirectUri to router.push without applying the isSafeRedirectUri check, allowing an organization or instance administrator to store a javascript or data URI that can execute in a user's browser when an affected login error path is reached. This issue is fixed in version 4.15.3. |
| CVE-2026-56308 | Capgo before 12.128.2 allows email address changes without requiring current password re-authentication or verification of the existing email address. An attacker with access to a valid session cookie or authenticated browser can change the account email to gain control of account recovery and bypass multi-factor authentication protections. |
| CVE-2026-59794 | In JetBrains TeamCity before 2026.1.2 stored XSS on the cloud profile page was possible via agent-reported data |
| CVE-2026-15490 | A security flaw has been discovered in RafyMrX TOKO-ONLINE-ROTI up to ddfe1cd587be0a0b5135d8b6e85cce2ec3aece99. Affected by this issue is some unknown functionality of the file proses/add.php. The manipulation of the argument kode_produk/kd_cs results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-55501 | 9Router is an AI router & token saver. Prior to 0.4.80, the dashboard login rate limiter in src/lib/auth/loginLimiter.js derives the client identity from the attacker-controlled X-Forwarded-For HTTP header, and src/app/api/auth/login/route.js uses that spoofable value for checkLock and recordFail. A remote attacker can rotate the X-Forwarded-For value on each login attempt to receive a fresh rate-limit bucket, bypass the 5-attempt threshold and progressive lockout durations, and |

| | |
|---|---|
| | perform unlimited brute-force attempts against the dashboard password. This issue is fixed in version 0.4.80. |
| CVE-2026-15491 | A weakness has been identified in RafyMrX TOKO-ONLINE-ROTI up to ddfe1cd587be0a0b5135d8b6e85cce2ec3aece99. This affects an unknown part. This manipulation causes missing authentication. The attack is possible to be carried out remotely. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15498 | A vulnerability was identified in sergomanov SmartHomeAdatum up to cf495353d81b680675eb8d9aa14a318aa45ce12c. This impacts an unknown function of the file users.php of the component Login. Such manipulation of the argument Login leads to sql injection. The attack may be launched remotely. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15497 | A vulnerability was determined in SonicCloudOrg sonic-agent up to 2.7.2. This affects an unknown function of the file sonic-server-controller/src/main/java/org/cloud/sonic/controller/controller/ExchangeController.java of the component JWT Authentication Filter. This manipulation causes code injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer. |
| CVE-2026-15134 | A vulnerability was determined in CodeAstro Simple Online Leave Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /SimpleOnlineLeave/index.php. Executing a manipulation of the argument email can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. |
| CVE-2026-61428 | PraisonAI AgentMail versions before 4.6.78 lack signature verification in webhook mode, allowing unauthenticated attackers to inject messages with spoofed sender addresses. Attackers can POST crafted message.received events to the webhook endpoint to inject arbitrary content into the agent and trigger replies to attacker-controlled addresses, bypassing sender allow/block lists. |
| CVE-2026-15597 | A security flaw has been discovered in SourceCodester Class and Exam Timetabling System 1.0/2.php. This affects an unknown function of the file /edit_exam2.php. Performing a manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. |
| CVE-2026-15479 | A vulnerability was found in H3C NX15 V100R017. Affected by this vulnerability is the function change_passwd of the file /api/login/modify of the component Administrator Password Modification Endpoint. The manipulation of the argument newPass results in weak password recovery. The attack may be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure. |
| CVE-2026-49789 | Stack-based buffer overflow in Windows NTFS allows an authorized attacker to elevate privileges locally. |
| CVE-2026-49790 | Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability |
| CVE-2026-15675 | A vulnerability was identified in code-projects Online Job Portal 1.0. The affected element is an unknown function of the file /Admin/EditUser.php. Such manipulation of the argument UserId leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used. |
| CVE-2026-15537 | A security flaw has been discovered in SourceCodester Online Book Store System 1.0. This vulnerability affects unknown code of the file admin/login.php. The manipulation of the argument Username results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. |
| CVE-2026-57028 | An Improper Restriction of Communication Channel to Intended Endpoints vulnerability in Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause license exhaustion. Due to an incorrect initialization, a process which should only be able to communicate internally within the device, can be reached over the network via an open port. This leads to unauthorized access to the license management. This issue affects all Junos OS Evolved versions before 23.2R2-EVO. |
| CVE-2026-55452 | Snipe-IT is an IT asset/license management system. Prior to 8.5.0, Actionlog::logaction() stores the request User-Agent header and ReportsController::postActivityReport() writes that value to the Activity Report CSV without formula escaping, allowing a low-privileged authenticated user to store a formula-like User-Agent that may execute when a report viewer opens the exported CSV in spreadsheet software. This issue is fixed in version 8.5.0. |
| CVE-2026-15541 | A flaw has been found in will-moss Isaiah up to 1.36.9. The impacted element is the function Server.Handle of the file app/server/server/server.go of the component Master Websocket Handler. Executing a manipulation of the argument Agent can lead to missing authorization. It is possible to launch the attack remotely. The pull request to fix this issue awaits acceptance. |
| CVE-2026-15542 | A vulnerability has been found in will-moss Isaiah up to 1.36.9. This affects an unknown function of the file app/main.go of the component Websocket Connection Authentication. The manipulation leads to improper authentication. The attack can be initiated remotely. The pull request to fix this issue awaits acceptance. |
| CVE-2026-15330 | A vulnerability was determined in zhayujie CowAgent up to 2.1.1. Impacted is the function _build_image_content/_download_to_data_url of the file agent/tools/vision/vision.py of the component Vision Tool. Executing a manipulation of the argument image can lead to server-side request forgery. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 2.1.2 is recommended to address this issue. This patch is called e85290cddcbb5ffc9c235927f4c92e5b4c3ec264. Upgrading the affected component is advised. |
| CVE-2026-13320 | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 15.7 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an authenticated user to execute arbitrary scripts in another user's browser session due to improper sanitization of user-supplied input. |
| CVE-2026-15488 | A vulnerability was determined in hcr707305003 shiroiAdmin 1.1/1.3. Affected is the function FileController::upload of the file app/common/controller/FileController.php. Executing a manipulation of the argument File can lead to unrestricted upload. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 1.4 is able to address this issue. This patch is called 3ecde28ea8a20a3840dbfefd6d6863ee79a83e70. It is suggested to upgrade the affected component. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-59214 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.10.0, Open WebUI runs client-side Python with Pyodide in a same-origin web worker, allowing stored chat payloads that use pyodide.http.pyfetch or the js module fetch and XMLHttpRequest APIs to issue authenticated same-origin requests when a victim clicks Run, which can reach admin-only endpoints and execute server-side code through configured tools. This issue is fixed in version 0.10.0. |
| CVE-2026- | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, a malicious second factor name on an attacker-controlled account was not escaped in the delete confirmation dialog, allowing stored cross-site scripting when an administrator impersonated that account. This issue is |

| | |
|---|---|
| 53963 | fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5. |
| CVE-2026-15482 | A weakness has been identified in Aster Telecom Azcall 10/11. This issue affects some unknown processing of the file /azcall/adm/gestao_loja/sis.php?t=consultar of the component HTTP Handler. Executing a manipulation of the argument nome/perfil/status can lead to sql injection. The attack may be performed from 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. |
| CVE-2026-59821 | LiteLLM is a proxy server (AI Gateway) to call LLM APIs in OpenAI (or native) format. Prior to 1.82.0-stable, LiteLLM's Custom Code Guardrails production create and update paths did not apply the same sandboxing and validation used by the test endpoint, allowing a privileged user with access to create or update guardrails to submit custom Python code that executed in the LiteLLM proxy environment and could expose secrets available to the process. This issue is fixed in version 1.82.0-stable. |
| CVE-2026-22660 | FlaskBB through 2.2.0, fixed in commit a5da9a5, contains a logic flaw vulnerability that allows authenticated administrators to delete all built-in authorization groups by exploiting a type mismatch in the bulk delete protection check. The bulk AJAX endpoint in the management views compares received JSON integer group IDs against string literals, causing the protection check to always pass, which allows deletion of all six built-in groups and destroys the forum's permission model, potentially rendering the site unusable. |
| CVE-2026-3576 | The Planyo Online Reservation System plugin for WordPress is vulnerable to Server-Side Request Forgery leading to Local File Inclusion in all versions up to, and including, 3.0. The ulap.php file acts as an AJAX proxy and is directly accessible without WordPress bootstrapping or any authentication. The send_http_post() function validates the host of the provided URL against an allowlist that includes 'localhost', but critically fails to validate the URL scheme/protocol. This makes it possible for unauthenticated attackers to supply a file:// URL (e.g., file://localhost/etc/passwd) which bypasses the host allowlist check because parse_url() returns 'localhost' as the host. The URL is then passed to curl_init() or fopen(), both of which support the file:// protocol, allowing the attacker to read arbitrary local files on the server and have their contents returned in the HTTP response. This can lead to disclosure of sensitive files such as /etc/passwd, wp-config.php (containing database credentials and authentication keys), and other server-side files. |
| CVE-2026-54801 | A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.20), SICORE Base system (All versions < V26.20.0). The affected application contains insufficient validation of authentication credentials when processing administrative account modifications through the web API. This could allow an authenticated attacker to bypass security controls and gain unauthorized elevated privileges. |
| CVE-2026-13430 | The Post Export Import with Media plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 1.13.1 via the import_media_file_secure function. This is due to insufficient file extension validation caused by a trailing-dot filename bypass, where the extension allow-list check in ajax_import_media_start() uses pathinfo() on the raw ZIP entry name (e.g., 'shell.php.'), which returns an empty string for the extension, causing the allow-list guard to be skipped and the file to be extracted to a temporary location, after which import_media_file_secure() copies it into the WordPress uploads directory without re-validating the extension. This makes it possible for authenticated attackers, with administrator-level access and above, to upload files that may be executable, which makes remote code execution possible. |
| CVE-2026-13441 | The EventPrime – Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'new_event_type_background_color' parameter in all versions up to, and including, 4.3.4.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with custom-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This requires the plugin's Guest Submissions setting (allow_submission_by_anonymous_user) to be enabled, which allows unauthenticated attackers to submit event types via the frontend form; when that setting is disabled, exploitation requires at minimum a subscriber-level authenticated account. |
| CVE-2026-54433 | In Roundcube Webmail before 1.6.17 and 1.7.x before 1.7.2, there is Stored Cross-Site Scripting (XSS) via a crafted plain-text email message. The attacker-controlled JavaScript executes within the victim's authenticated session simply by opening or previewing the message (zero-click). |
| CVE-2026-13114 | The Motors – Car Dealership & Classified Listings Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content and User Biographical Info in all versions up to, and including, 1.4.112 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-59521 | Deserialization of Untrusted Data vulnerability in ShapedPlugin LLC Real Testimonials testimonial-free allows Object Injection.This issue affects Real Testimonials: from n/a through <= 3.1.15. |
| CVE-2026-9253 | The WP Cost Estimation & Payment Forms Builder (E&P Forms) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'customerInfos' parameter in all versions up to, and including, 10.5.97 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-13378 | The Form Vibes – Database Manager for Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Contact Form 7 Form Field in all versions up to, and including, 1.5.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-15000 | The Connect Contact Form 7 and Mailchimp plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Mailchimp Merge Field Values in all versions up to, and including, 0.9.78.06 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The injected payload is only triggered when a privileged user (Administrator) performs a Contact Lookup for the email address submitted via the CF7 form, meaning execution is deferred until an administrator interacts with the affected entry. |
| CVE-2026-8848 | The Popup Maker – Boost Sales, Conversions, Optins, Subscribers with the Ultimate WP Popup Builder plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.22.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with editor-level access and above, to install and activate an arbitrary plugin from an attacker-controlled URL, leading to remote code execution. Exploitation requires that a valid Popup Maker Pro license is active on the target site and that Popup Maker Pro is not yet installed, as these conditions are necessary for the legacy v1/connect/info endpoint to issue the bearer token used to satisfy the install endpoint's only non-spoofable validation check. |
| CVE-2026-60091 | PraisonAI before 4.6.78 contains an unauthenticated server-side request forgery vulnerability in the Jobs API /api/v1/runs endpoint. The webhook_url parameter is validated at request time but re-resolved at connection time, allowing attackers to use DNS rebinding to reach internal services with a blind SSRF attack. |
| CVE-2026-24699 | An OS command injection vulnerability exists in the sub_34984() function of the "rc" binary in Cisco RV130/RV130W with firmware 1.0.3.55 and RV110W routers with firmware 1.2.2.5 / 1.2.2.8. The lan_ipv6_prefixlen configuration parameter is not properly sanitized, which could allow an authenticated remote attacker to execute arbitrary OS commands with root privileges. |
| CVE-2026-10698 | Improper Neutralization of Special Elements in Data Query Logic vulnerability in Progress MOVEit Transfer (Custom Reports modules). This issue affects MOVEit Transfer: from 2025.0.0 before 2025.0.8, from 2025.1.0 before 2025.1.4, from 2026.0.0 before 2026.0.1. |
| CVE- | An OS command injection vulnerability exists in the start_bonjour() function of the "rc" binary in Cisco RV130/RV130W with firmware 1.0.3.55 and RV110W routers |

| | |
|---|---|
| 2026-24697 | with firmware 1.2.2.5 / 1.2.2.8. The wan_hostname configuration parameter is not properly sanitized, which could allow an authenticated remote attacker to execute arbitrary OS commands with root privileges. |
| CVE-2026-57407 | Server-Side Request Forgery (SSRF) vulnerability in WP Swings PDF Generator for WordPress pdf-generator-for-wp allows Server Side Request Forgery.This issue affects PDF Generator for WordPress: from n/a through <= 1.6.2. |
| CVE-2026-6820 | The VikBooking Hotel Booking Engine & PMS plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'email' parameter in all versions up to, and including, 1.8.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-24698 | An OS command injection vulnerability exists in the save_syslog_to_file() function of the "httpd" binary in Cisco RV130/RV130W with firmware 1.0.3.55 and RV110W routers with firmware 1.2.2.5 / 1.2.2.8. The model_name configuration parameter is not properly sanitized, which could allow an authenticated remote attacker to execute arbitrary OS commands with root privileges. |
| CVE-2026-6939 | The CorvusPay WooCommerce Payment Gateway plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'approval_code' parameter in all versions up to, and including, 2.7.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The unauthenticated REST endpoint POST /wp-json/corvuspay/success/ is registered with permission_callback set to __return_true, and although a signature validation step exists it only logs the result without halting execution, meaning an attacker can supply a completely arbitrary signature and have a malicious approval_code stored in the database unchallenged. |
| CVE-2026-59721 | Hoppscotch is an open source API development ecosystem. Prior to 2026.6.0, the updateInfraConfigs GraphQL mutation in admin/infra.resolver.ts accepts an attacker-controlled MAILER_SMTP_URL value, and validateSMTPUrl in utils.ts permits path, query, or fragment content that nodemailer parses into sendmail transport options, allowing an admin to execute arbitrary commands as root in the backend container after restart and mail sending. This issue is fixed in version 2026.6.0. |
| CVE-2026-24700 | An OS command injection vulnerability exists in the start_lltd() function of the "rc" binary in Cisco RV130/RV130W with firmware 1.0.3.55 and RV110W routers with firmware 1.2.2.5 / 1.2.2.8. The machine_name configuration parameter is not properly sanitized, which could allow an authenticated remote attacker to execute arbitrary OS commands with root privileges. |
| CVE-2026-6818 | The VikBooking Hotel Booking Engine & PMS plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'special_requests' parameter in all versions up to, and including, 1.8.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-1667 | The SEO Plugin by Squirrly SEO plugin for WordPress is vulnerable to Arbitrary Post Creation and Stored Cross-Site Scripting in all versions up to, and including, 14.0.0 due to a leak of an API token and insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to create arbitrary posts, and, if the Advanced Custom Fields plugin is installed and activated, inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-44161 | Fluentd collects events from various data sources and writes them to files, RDBMS, NoSQL, IaaS, SaaS, Hadoop and so on. Prior to 1.19.3, the Fluentd out_http output plugin allows placeholders such as ${tag} in the endpoint configuration parameter, and if a placeholder value is derived from untrusted input an attacker can control the destination hostname of outbound HTTP requests and force requests to arbitrary internal services. This issue is fixed in version 1.19.3. |
| CVE-2026-62643 | In Roundcube Webmail before 1.6.17 and 1.7.x before 1.7.2, insufficient Cascading Style Sheets (CSS) sanitization in HTML e-mail messages may lead to SSRF or Information Disclosure, e.g., if stylesheet links point to local network hosts. NOTE: this issue exists because of insufficient fixes for CVE-2026-35540 and CVE-2026-48843. |
| CVE-2026-0286 | A command injection vulnerability in the management plane of Palo Alto Networks PAN-OS® software enables an authenticated administrator to execute arbitrary OS commands as root. The security risk posed by this issue is significantly minimized when CLI access is restricted to a limited group of administrators. This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series). Cloud NGFW and Prisma Access® are not impacted by this vulnerability. |
| CVE-2026-0283 | An authentication bypass vulnerability in Large Scale VPN ( LSVPN) functionality of Palo Alto Networks PAN-OS software allows an attacker with network access to bypass security restrictions and establish an unauthorized site-to-site VPN connection. Panorama, Cloud NGFW, and Prisma® Access are not impacted by this vulnerability. |
| CVE-2026-0280 | An IPv6 packet processing vulnerability in the dataplane of Palo Alto Networks PAN-OS® software enables an unauthenticated attacker to bypass firewall security policy enforcement, allowing network traffic that should be blocked to reach protected services. Cloud NGFW and Panorama are not impacted by this vulnerability. |
| CVE-2026-57372 | Server-Side Request Forgery (SSRF) vulnerability in denishua WPJAM Basic wpjam-basic allows Server Side Request Forgery.This issue affects WPJAM Basic: from n/a through <= 7.0. |
| CVE-2026-61343 | LibreBooking's email template editor save action passes the submitted template name directly into the destination file path, allowing a remote attacker with administrator credentials to write an arbitrary file outside the template directory and execute code. Fixed in 5.1.0. |
| CVE-2026-53448 | Coturn is a free open source implementation of TURN and STUN Server. Prior to 4.12.0, the coturn HTTPS admin panel passes HTTP query parameters directly into SQL queries via snprintf string interpolation without sanitization. The is_secure_string filter that protects the STUN protocol path is not applied to the admin panel's delete-user, delete-secret, and delete-IP operations, so an authenticated admin can inject arbitrary SQL through the du, ds, and dip parameters, gaining full database control and potentially OS-level access via PostgreSQL COPY TO PROGRAM. This issue is fixed in version 4.12.0. |
| CVE-2026-15298 | The TelSender plugin for WordPress is vulnerable to DOM-Based Cross-Site Scripting in all versions up to, and including, 1.14.14. This is due to insufficient input sanitization when processing Telegram API responses containing attacker-controlled chat titles. This makes it possible for unauthenticated attackers to inject malicious scripts via Telegram chat titles that execute when an administrator opens the TelSender settings page and clicks the "Tested" button. |
| CVE-2026-57728 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UX-themes Flatsome flatsome allows Reflected XSS.This issue affects Flatsome: from n/a through <= 3.20.5. |
| CVE-2026-57718 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) unlimited-elements-for-elementor allows Reflected XSS.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through <= 2.0.12. |
| CVE-2026-57725 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeum Kirki kirki allows Stored XSS.This issue affects Kirki: from n/a through <= 6.0.11. |

| | |
|---|---|
| CVE-2026-57715 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPManageNinja Fluent CRM fluent-crm allows Reflected XSS.This issue affects Fluent CRM: from n/a through <= 3.1.7. |
| CVE-2026-57733 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Cloud Library td-cloud-library allows DOM-Based XSS.This issue affects tagDiv Cloud Library: from n/a through <= 3.9.4. |
| CVE-2026-57376 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Element Invader ElementInvader Addons for Elementor elementinvader-addons-for-elementor allows DOM-Based XSS.This issue affects ElementInvader Addons for Elementor: from n/a through <= 1.4.3. |
| CVE-2026-57740 | Missing Authorization vulnerability in AcyMailing Newsletter Team AcyMailing SMTP Newsletter acymailing allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AcyMailing SMTP Newsletter: from n/a through <= 10.11.1. |
| CVE-2026-61442 | PraisonAI Platform (praisonai-platform) before 0.1.9 fails to enforce owner/admin authorization on the PATCH routes for projects, issues, and agents, which only require workspace-member role. A workspace member can modify owner-created records; for projects, a member can reassign lead_id to their own user id and then delete the owner-created project, bypassing the delete route's owner/admin permission check. |
| CVE-2026-57734 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Composer td-composer allows Reflected XSS.This issue affects tagDiv Composer: from n/a through <= 5.4.3. |
| CVE-2026-57379 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPPOOL FormyChat social-contact-form allows Stored XSS.This issue affects FormyChat: from n/a through <= 2.15.3. |
| CVE-2026-57368 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme Jobmonster noo-jobmonster allows Reflected XSS.This issue affects Jobmonster: from n/a through <= 4.8.5. |
| CVE-2026-57363 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in QuantumCloud ChatBot chatbot allows Stored XSS.This issue affects ChatBot: from n/a through <= 8.3.7. |
| CVE-2026-39903 | Simple Machines Forum 2.1 prior to commit 7d048f8 and 3.0 prior to commit a7875e8 contains an authorization bypass vulnerability in Sources/Actions/AttachmentApprove.php where a single-character operator error causes the permission check to always pass regardless of user permissions. An authenticated low-privileged user can approve, reject, or delete any pending attachments on any board without holding the required approve_posts permission, bypass moderation queues for their own uploads, and enumerate and delete other users' pending attachments. |
| CVE-2026-57712 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPZOOM WPZOOM Portfolio wpzoom-portfolio allows Reflected XSS.This issue affects WPZOOM Portfolio: from n/a through <= 1.4.29. |
| CVE-2026-57741 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AcyMailing Newsletter Team AcyMailing SMTP Newsletter acymailing allows Stored XSS.This issue affects AcyMailing SMTP Newsletter: from n/a through <= 10.11.0. |
| CVE-2026-57396 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Flintop Free Gifts for WooCommerce free-gifts-for-woocommerce allows Stored XSS.This issue affects Free Gifts for WooCommerce: from n/a through <= 13.1.0. |
| CVE-2026-57380 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hupe13 Extensions for Leaflet Map extensions-leaflet-map allows DOM-Based XSS.This issue affects Extensions for Leaflet Map: from n/a through <= 5.1. |
| CVE-2026-57405 | Missing Authorization vulnerability in themehunk Open Shop open-shop allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Open Shop: from n/a through <= 1.7.1. |
| CVE-2026-58410 | ChurchCRM is an open-source church management system. Prior to version 7.4.0, there was an authorization flaw in the family-scoped endpoints which allowed low-privileged users to read and modify other families' records. An authenticated non-admin user with EditSelf access can supply another family's `familyId` and access records outside their own family scope. The backend trusts the attacker-controlled `familyId` and loads the corresponding family entity by ID without verifying that the requested family belongs to the current user. If the same user also has Notes permission, they can create notes on another family's record. This breaks the intended EditSelf scope and allows access to unrelated congregation records. This issue has been fixed in version 7.4.0. |
| CVE-2026-57388 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themefic Hydra Booking hydra-booking allows Stored XSS.This issue affects Hydra Booking: from n/a through <= 1.1.44. |
| CVE-2026-57415 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Codemenschen Gift Vouchers gift-voucher allows Stored XSS.This issue affects Gift Vouchers: from n/a through <= 4.7.0. |
| CVE-2026-57411 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aman CF7 Views – Complete Entry Management for Contact Form 7 cf7-views allows DOM-Based XSS.This issue affects CF7 Views – Complete Entry Management for Contact Form 7: from n/a through <= 3.2.2. |
| CVE-2026-55880 | OpenReplay is a self-hosted session replay suite. In 1.27.0 and earlier, three dashboard and note mutation functions ran their SQL without the ownership predicate that their sibling read and edit functions use: notes.delete filtered only on note id and project id, while dashboards.update_widget and dashboards.remove_widget filtered only on dashboard id and widget id, allowing any authenticated member to delete another user's private session notes and remove or rewrite widgets on another user's private dashboards. |
| CVE-2026-57409 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RealMag777 Active Products Tables for WooCommerce profit-products-tables-for-woocommerce allows DOM-Based XSS.This issue affects Active Products Tables for WooCommerce: from n/a through <= 1.1.0. |

| | |
|---|---|
| CVE-2026-62191 | OpenClaw versions 2026.6.6 before 2026.6.9 contain an authorization bypass vulnerability in message mutation handling that allows lower-trust callers to perform actions requiring stronger authorization checks. Attackers can exploit misconfigured input paths to skip requester authorization and execute privileged operations when the affected feature is enabled and reachable. |
| CVE-2026-57416 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SiteGround SiteGround Email Marketing siteground-email-marketing allows Stored XSS.This issue affects SiteGround Email Marketing: from n/a through <= 1.7.5. |
| CVE-2026-57403 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Milan Petrovic GD Security Headers gd-security-headers allows Reflected XSS.This issue affects GD Security Headers: from n/a through <= 1.8. |
| CVE-2026-57394 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tribulant Software Newsletters newsletters-lite allows Reflected XSS.This issue affects Newsletters: from n/a through <= 4.14. |
| CVE-2026-57399 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Proxy & VPN Blocker Proxy & VPN Blocker proxy-vpn-blocker allows Stored XSS.This issue affects Proxy & VPN Blocker: from n/a through <= 3.5.8. |
| CVE-2026-57398 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebCodingPlace Real Estate Manager Pro real-estate-manager-pro allows Reflected XSS.This issue affects Real Estate Manager Pro: from n/a through <= 12.8.3. |
| CVE-2026-12275 | The Tutor LMS WordPress plugin before 3.9.13 does not, in its Droip and Kirki page-builder integration, perform the enrollment, purchase, and private-course capability checks it enforces in its core course handler, allowing authenticated users with subscriber-level access to enroll in paid or private courses without authorization, read private course content, and mark arbitrary courses as completed, on sites where the Droip or Kirki integration is active. |
| CVE-2026-62189 | OpenClaw versions before 2026.6.9 contain a symlink following vulnerability in the mirror sync feature that allows lower-trust callers to perform actions requiring stronger authorization. Attackers can exploit remote symlink parents to bypass policy checks and authorization boundaries when the feature is enabled and reachable. |
| CVE-2026-57387 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in picu picu picu allows Stored XSS.This issue affects picu: from n/a through <= 3.5.1. |
| CVE-2026-57383 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eyecix JobSearch wp-jobsearch allows Stored XSS.This issue affects JobSearch: from n/a through <= 3.2.9. |
| CVE-2026-57381 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Property Hive PropertyHive propertyhive allows Reflected XSS.This issue affects PropertyHive: from n/a through <= 2.2.3. |
| CVE-2026-57816 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FunnelKit Funnel Builder by FunnelKit funnel-builder allows Reflected XSS.This issue affects Funnel Builder by FunnelKit: from n/a through <= 3.15.0.8. |
| CVE-2026-57745 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in stmcan RT-Theme 18 \| Extensions rt18-extensions allows Reflected XSS.This issue affects RT-Theme 18 \| Extensions: from n/a through <= 2.5. |
| CVE-2026-57708 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CRM Perks Contact Form Entries contact-form-entries allows Reflected XSS.This issue affects Contact Form Entries: from n/a through <= 1.5.2. |
| CVE-2026-57706 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dokan, Inc. Dokan dokan-lite allows Reflected XSS.This issue affects Dokan: from n/a through <= 5.0.6. |
| CVE-2026-57695 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dan Rossiter Document Gallery document-gallery allows Reflected XSS.This issue affects Document Gallery: from n/a through <= 5.1.0. |
| CVE-2026-57382 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mitchell Bennis Simple File List simple-file-list allows Reflected XSS.This issue affects Simple File List: from n/a through <= 6.3.8. |
| CVE-2026-57814 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPMU DEV - Your All-in-One WordPress Platform Forminator forminator allows DOM-Based XSS.This issue affects Forminator: from n/a through <= 1.55.0.1. |
| CVE-2026-59516 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Room 34 Creative Services, LLC ICS Calendar ics-calendar allows Reflected XSS.This issue affects ICS Calendar: from n/a through <= 12.1.1. |
| CVE-2026-57417 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RexTheme Cart Lift cart-lift allows Stored XSS.This issue affects Cart Lift: from n/a through <= 3.1.57. |
| CVE-2026-61956 | Cross-Site Request Forgery (CSRF) vulnerability in hamsalam همگام سازی ووکامرس و باسلام – ووسلام sync-basalam allows Cross Site Request Forgery.This issue affects همگام سازی ووکامرس و باسلام – ووسلام: from n/a through <= 1.9.1. |
| CVE-2026-57668 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Basix NEX-Forms nex-forms-express-wp-form-builder allows Stored XSS.This issue affects NEX-Forms: from n/a through <= 9.2.2. |

| | |
|---|---|
| CVE-2026-57423 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kofi Mokome Message Filter for Contact Form 7 cf7-message-filter allows Reflected XSS.This issue affects Message Filter for Contact Form 7: from n/a through <= 1.6.3.8. |
| CVE-2026-57422 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VillaTheme Bopo – WooCommerce Product Bundle Builder bopo-woo-product-bundle-builder allows Reflected XSS.This issue affects Bopo – WooCommerce Product Bundle Builder: from n/a through <= 1.2.0. |
| CVE-2026-57421 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CRM Perks CRM Perks Forms crm-perks-forms allows Reflected XSS.This issue affects CRM Perks Forms: from n/a through <= 1.1.7. |
| CVE-2026-55460 | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, an authenticated non-admin user with users.view and users.edit but without users.delete can directly POST to /users/bulksave with delete_user=1 because BulkUsersController::destroy() authorizes only update, allowing the user to soft-delete another non-admin user. This issue is fixed in version 8.6.2. |
| CVE-2026-57732 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Opt-In Builder td-subscription allows DOM-Based XSS.This issue affects tagDiv Opt-In Builder: from n/a through <= 1.7.4. |
| CVE-2026-57369 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themifyme Themify Builder themify-builder allows Reflected XSS.This issue affects Themify Builder: from n/a through <= 7.7.4. |
| CVE-2026-50354 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally. |
| CVE-2026-59219 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.0 before 0.10.0 with Redis configured, Socket.IO connect, user-join, join-channels, join-note, and the terminal websocket first-message authentication used decode_token without the Redis-backed is_valid_token revocation check, allowing revoked JWTs to continue authenticating realtime connections. This issue is fixed in version 0.10.0. |
| CVE-2026-49791 | Improper link resolution before file access ('link following') in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to elevate privileges locally. |
| CVE-2026-55212 | Pimcore is an Open Source Data & Experience Management Platform. Prior to 2025.4.6 and 2026.1.6, the Studio API class definition creation endpoint POST /pimcore-studio/api/class/definition/configuration-view/detail/create is guarded by the objects permission instead of the classes permission, allowing a standard editor-level user to create class definitions without admin privileges. Class definition creation generates new database tables and PHP class files on the server, and missing API-layer UID format validation allows malformed UIDs to reach model-layer validation and return internal exceptions. This issue is fixed in versions 2025.4.6 and 2026.1.6. |
| CVE-2026-41122 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain a stored cross-site scripting vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability. Exploitation may lead to information disclosure, session theft, or client-side request forgery. |
| CVE-2026-59261 | OpenClaw before 2026.5.28 contains a credential exposure vulnerability where workspace dotenv files can override provider credentials. Attackers with lower-trust access to configured input paths can expose sensitive data and credentials that should remain within trusted boundaries. |
| CVE-2026-31982 | An Open Redirect vulnerability was discovered in the SAML Single Sign-On functionality due to insufficient validation of a user-controlled redirection parameter. An unauthenticated attacker can craft a request to the SAML sign-in endpoint and poison the cached SAML redirection for other users who subsequently initiate SAML Single Sign-On, enabling phishing and credential-theft attacks, as well as disrupting SAML authentication for all affected users. |
| CVE-2026-55651 | Easy!Appointments is a self hosted appointment scheduler. In version 1.5.2, an Excessive Data Exposure vulnerability in the customers search endpoint allows an authenticated user to obtain appointment hashes belonging to other users. Using these hashes, an attacker can modify or delete appointments of other providers, resulting in an Appointments Takeover. Version 1.6.0 fixes the issue. |
| CVE-2026-56193 | Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally. |
| CVE-2026-50428 | Out-of-bounds read in Windows Container Isolation FS Filter Driver (unionfs.sys) allows an authorized attacker to disclose information locally. |
| CVE-2026-0281 | An information disclosure vulnerability in Palo Alto Networks PAN-OS® software enables an unauthenticated attacker with network access to the management web interface to obtain web session tokens. This requires a legitimate user to first click on a malicious link provided by the attacker. The security risk posed by this issue is minimized by restricting access to the management web interface to only trusted internal IP addresses according to our recommended best practice deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series). Cloud NGFW and Prisma® Access are not impacted by this vulnerability. |
| CVE-2026-49165 | Use of uninitialized resource in Microsoft Windows App Store allows an authorized attacker to disclose information locally. |
| CVE-2026-14372 | The Bit Form – Contact Form, Payment Forms, Multi Step Forms, Calculator & Custom Form Builder plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the deleteFiles function in all versions up to, and including, 3.1.1 This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config). |
| CVE-2026-59691 | A heap buffer overflow vulnerability was found in GStreamer's rfbsrc plugin. When a client connects to a malicious RFB/VNC server that advertises a 16bpp framebuffer and sends Hextile-encoded updates, the Hextile background fill path writes 32-bit pixel values into a buffer allocated for 16-bit pixels. This type mismatch causes an out-of-bounds heap write that can lead to denial of service (process crash) and potential memory corruption. |
| CVE- | Langroid is a framework for building large-language-model-powered applications. Prior to version 0.64.0, Langroid's `ReadFileTool` and `WriteFileTool` appear to treat `curr_dir` as the intended working-directory boundary for file operations. However, the tools only change the process working directory to `curr_dir` and |

| | |
|---|---|
| 2026-50181 | then operate on the user-supplied `file_path` without resolving and enforcing that the final path remains inside `curr_dir`. As a result, a tool caller can supply path traversal sequences such as `../secret.txt` to read files outside the configured current directory, or `../written_by_tool.txt` to write files outside that directory. This can impact applications that expose Langroid file tools to an LLM agent, user-controlled tool call, or delegated coding/documentation agent while relying on `curr_dir` to restrict file access to a project/workspace directory. Version 0.64.0 patches the issue. |
| CVE-2026-59206 | n8n is an open source workflow automation platform. Prior to 1.123.61, 2.27.4, and, 2.28.1, an authenticated user with the default workflow:create permission could pollute Object.prototype through a crafted workflow saved, updated, or imported via the workflow API, allowing unauthenticated requests to be treated as a privileged user and exposing user and project listing endpoints. This issue is fixed in versions 1.123.61, 2.27.4, and 2.28.1. |
| CVE-2026-35210 | OpenCTI is an open source platform for managing cyber threat intelligence knowledge and observables. Prior to 7.260326.0, an authorization bypass vulnerability in OpenCTI allows any authenticated user with KNOWLEDGE_KNUPDATE permission to bypass Confidence Level validation and Object Marking restrictions by injecting the synchronized-upsert: true HTTP header, enabling attackers to downgrade confidence levels, remove security markings such as TLP:RED, manipulate relationships, and affect STIX object types including Indicators, ThreatActors, Malware, and Reports. This issue is fixed in version 7.260326.0. |
| CVE-2026-58213 | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.1 and 2.12.9, an MQTT client could include protocol control characters in subscription filters that were later forwarded as NATS protocol data to route or leafnode connections, corrupting the forwarded protocol stream and allowing injection of unintended NATS protocol operations. This issue is fixed in versions 2.14.1 and 2.12.9. |
| CVE-2026-50451 | Missing authentication for critical function in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to elevate privileges locally. |
| CVE-2026-54528 | JupyterLab Git is a Git extension for JupyterLab. Prior to 0.54.0, jupyterlab-git uses fnmatch.fnmatchcase() in GitHandler.prepare() in jupyterlab_git/handlers.py to enforce excluded_paths, allowing an authenticated user on a case-insensitive filesystem to vary URL path casing and read excluded directories. This issue is fixed in version 0.54.0. |
| CVE-2026-55144 | Missing cryptographic step in Windows CryptoAPI allows an authorized attacker to perform tampering locally. |
| CVE-2026-10671 | In Zephyr's kernel pipe implementation, the userspace syscall verifier z_vrfy_k_pipe_init() in kernel/pipe.c used K_SYSCALL_OBJ() (which requires the kernel object to already be initialized) instead of K_SYSCALL_OBJ_NEVER_INIT() (which rejects an already-initialized object). As a result, on CONFIG_USERSPACE builds an unprivileged user thread that has been granted access to a k_pipe object can invoke the k_pipe_init syscall to re-initialize a pipe that is already in use. z_impl_k_pipe_init() unconditionally resets the ring buffer, sets pipe->waiting to 0, and re-initializes both wait queues (z_waitq_init on pipe->data and pipe->space) without waking or accounting for threads currently blocked on the pipe. Any thread already pended in k_pipe_read()/k_pipe_write() is left orphaned: still marked pending with pended_on pointing at the cleared wait queue and with stale qnode_dlist links into the (now re-initialized) embedded list head. When such an orphaned waiter is later timed out or woken, the scheduler calls sys_dlist_remove() on its stale node, writing through dangling prev/next pointers into kernel wait-queue/scheduler structures, causing list corruption (an attacker-driven invalid kernel write), lost wakeups, indefinitely blocked threads, and silent data loss. The flaw lets a deprivileged user thread corrupt the state of a kernel object shared with other threads/partitions. The fix switches the verifier to K_SYSCALL_OBJ_NEVER_INIT(), matching the existing k_msgq_init verifier, so a user thread can no longer re-initialize a live pipe. The vulnerable code shipped in v4.1.0 and remained through v4.4.0. |
| CVE-2026-15515 | A security vulnerability has been detected in Tencent PC Manager 18.1.30242.301. This issue affects some unknown processing in the library qmudisk64.sys of the component QMUDisk Driver. The manipulation leads to uncontrolled search path. The attack must be carried out locally. The attack is considered to have high complexity. The exploitability is assessed as difficult. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-49805 | Improper access control in Windows Win32K allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50392 | Use after free in Windows Secure Kernel Mode allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50393 | Use after free in Windows Kernel-Mode Drivers allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50390 | Access of resource using incompatible type ('type confusion') in Windows Kernel allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50322 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50396 | Use after free in Windows Kernel-Mode Drivers allows an authorized attacker to elevate privileges locally. |
| CVE-2026-49802 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges locally. |
| CVE-2026-49803 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows AppX Deployment Service allows an authorized attacker to elevate privileges locally. |
| CVE-2026-54989 | Use after free in Quality Windows Audio/Video Experience (QWAVE) service allows an authorized attacker to elevate privileges locally. |
| CVE-2026-59948 | Composer is a dependency Manager for the PHP language. Prior to 2.2.29 and 2.10.2, a maliciously crafted package from an untrusted repository other than Packagist.org or Private Packagist can cause Composer to write attacker-controlled files outside the vendor directory and outside the project during install or update by using an invalid package name that is not correctly validated before dependency-resolution results are written or installed. This issue is fixed in versions 2.2.29 and 2.10.2. |

| | |
|---|---|
| CVE-2026-50372 | Buffer over-read in Windows Redirected Drive Buffering allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50345 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally. |
| CVE-2026-48571 | Use after free in Windows App Installer allows an authorized attacker to elevate privileges locally. |
| CVE-2026-48572 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows App Installer allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50371 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows LUAFV allows an authorized attacker to elevate privileges locally. |
| CVE-2026-49784 | Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Windows App Store allows an authorized attacker to elevate privileges locally. |
| CVE-2026-49162 | Use after free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally. |
| CVE-2026-49183 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Clipboard Server allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50359 | Use after free in Microsoft XML Core Services allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50358 | Use after free in Windows Media allows an authorized attacker to elevate privileges locally. |
| CVE-2026-49806 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50307 | Use after free in Windows TCP/IP allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50325 | Improper access control in Windows Win32K allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50323 | Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally. |
| CVE-2026-54996 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50452 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an unauthorized attacker to elevate privileges over a network. |
| CVE-2026-54129 | Use after free in Windows Hyper-V allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50449 | Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally. |
| CVE-2026-54111 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges locally. |
| CVE-2026-56254 | In @capgo/capacitor-updater (Cap-go/capgo) before 12.128.2, the end-to-end encryption scheme distributes the private key to each device that downloads the app. Because the public key can be derived from the private key, an attacker performing a man-in-the-middle attack or compromising the Capgo server can create a validly signed update bundle and cause devices to install an update not produced by the original app maker. |
| CVE-2026-50384 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Clip Service allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50356 | Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Windows App Store allows an authorized attacker to elevate privileges locally. |
| CVE- | |

| | |
|---|---|
| 2026-50397 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally. |
| CVE-2026-58526 | Use after free in Windows Storage allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50348 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an unauthorized attacker to elevate privileges over a network. |
| CVE-2026-56297 | FreeRDP before 3.22.0 contains a use-after-free vulnerability in dvcman_channel_close and dvcman_call_on_receive due to improper synchronization of channel_callback access. A malicious RDP server can trigger a race condition by sending DYNVC_DATA and DYNVC_CLOSE messages concurrently, causing heap-use-after-free in the drdynvc client thread and potentially enabling remote code execution or denial of service. |
| CVE-2026-50410 | Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50406 | Use after free in Windows Backup Engine allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50297 | Improper access control in Windows Win32K allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50296 | Use after free in Graphics Kernel allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50403 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50404 | Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Media allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50299 | Integer overflow or wraparound in Windows Storage Spaces Direct allows an unauthorized attacker to execute code with a physical attack. |
| CVE-2026-59804 | Midscene Bridge Server through 1.10.3, fixed in commit 86f4118, contains a missing authentication and CORS misconfiguration vulnerability that allows unauthenticated remote attackers to hijack active bridge sessions by opening a cross-origin WebSocket connection to the local Socket.IO server, which performs no Origin header validation and requires no authentication token. Attackers can connect from any web page visited by the victim to seize the single-client slot, intercept and inject automation commands, exfiltrate command-payload data, or unconditionally terminate the server by supplying the MIDSCENE_BRIDGE_SIGNAL_KILL query parameter. |
| CVE-2026-59208 | n8n is an open source workflow automation platform. Prior to 2.27.4 and from 2.28.0 prior to 2.28.1, n8n instances configured with more than one trusted token-exchange issuer resolved external identities to local accounts using only the JWT sub claim and ignored the iss claim, allowing an attacker with a valid token from one trusted issuer and a sub matching a victim under another issuer to authenticate as that victim. This issue is fixed in versions 2.27.4 and 2.28.1. |
| CVE-2026-49168 | Integer overflow or wraparound in Windows Storage Spaces Direct allows an unauthorized attacker to elevate privileges with a physical attack. |
| CVE-2026-58208 | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.3 and 2.12.12, a WebSocket listener could route requests for the MQTT-over-WebSocket path into MQTT handling even when MQTT was not configured, allowing an unauthenticated client with access to the WebSocket listener to reach uninitialized MQTT state and crash the server process. This issue is fixed in versions 2.14.3 and 2.12.12. |
| CVE-2026-59807 | Composio SDK before 0.2.32-beta.283 contains a path validation bypass vulnerability that allows attackers to read and exfiltrate sensitive files by exploiting a missing assertSafeFileUploadPath check in the readFileFromDisk function within tool-file-uploads.ts. Attackers can exploit prompt injection to manipulate file_uploadable parameters to reference sensitive paths such as SSH private keys, causing the CLI to upload credential files to attacker-controlled storage. |
| CVE-2026-54132 | Heap-based buffer overflow in Windows Kernel allows an unauthorized attacker to elevate privileges with a physical attack. |
| CVE-2026-50298 | Integer overflow or wraparound in Windows Spaceport.sys allows an unauthorized attacker to elevate privileges with a physical attack. |
| CVE-2026-55689 | OpenFGA is an authorization/permission engine built for developers. Prior to 1.18.0, OpenFGA's OIDC authenticator skipped JWT audience validation when authn.method was set to oidc, authn.oidc.issuer was configured, and authn.oidc.audience was not set, allowing a token minted for an unrelated service by the same identity provider to authenticate to OpenFGA. This issue is fixed in 1.18.0. |
| CVE-2026-57216 | RabbitMQ is a messaging and streaming broker. Prior to 3.13.15, 4.0.20, 4.1.11, and 4.2.6, AMQP 0-9-1, AMQP 1.0, and Stream Protocol authentication can allow a loopback-restricted user such as guest to connect remotely when traffic is accepted through a trusted PROXY-protocol path and the backend listener is loopback-bound because the loopback check uses the listener-side socket address instead of the real client source. This issue is fixed in versions 3.13.15, 4.0.20, 4.1.11, and 4.2.6. |
| CVE-2026-8595 | A user with Editor permissions can craft a dashboard whose table (TableNG) panel contains a malicious field name that executes as a script in the browser of any user who views the dashboard (stored cross-site scripting). |
| CVE-2026- | A protection mechanism failure in the Code 27 Companion Hub allows an attacker with physical access to completely bypass kiosk restrictions via a factory reset |

| | |
|---|---|
| 36028 | |
| CVE-2026-50426 | Relative path traversal in DNS Server allows an authorized attacker to execute code over an adjacent network. |
| CVE-2026-55885 | Grav is a file-based Web platform. Prior to 1.7.53, an authenticated administrator with backup permissions can download a ZIP archive containing the full Grav installation root, including user/accounts/admin.yaml with the administrator password hash and user/config with site configuration, through the backup download endpoint protected only by the session-static admin-nonce URL parameter. This issue is reported as fixed in version 1.7.53. |
| CVE-2026-36027 | An issue in Code27 Companion Hub SQ3A.220705.003.A1 allows a physically proximate attacker to execute arbitrary code via the USB debugging (ADB) and Android Debug Bridge components |
| CVE-2026-0275 | A local privilege escalation vulnerability in Palo Alto Networks Prisma® Browser allows a locally authenticated administrator with access to the macOS local filesystem to perform actions on the device with root privileges. This issue only affects Prisma® Browser on macOS. |
| CVE-2025-40945 | A vulnerability has been identified in COMOS V10.4.5 (All versions < V10.4.5.0.2), COMOS V10.6 (All versions < V10.6.1), Designcenter NX (All versions < V2512.7000), Simcenter 3D (All versions < V2512.7000), Simcenter Femap V2506 (All versions < V2506.0003), Simcenter Femap V2512 (All versions < V2512.0002), Simcenter Nastran (All versions < V2606), Simcenter STAR-CCM+ (All versions < V2606), Solid Edge SE2025 (All versions < V225.0 Update 13), Solid Edge SE2026 (All versions < V226.0 Update 04), Teamcenter Visualization V2412 (All versions < V2412.0012), Teamcenter Visualization V2506 (All versions < V2506.0009), Teamcenter Visualization V2512 (All versions < V2512.2605), Tecnomatix Plant Simulation V2404 (All versions < V2404.0022), Tecnomatix Plant Simulation V2504 (All versions < V2504.0010), Tecnomatix Process Simulate (All versions < V2606). Untrusted search path in IAM Client SDK may allow an authenticated user to potentially enable escalation of privilege via local access. |
| CVE-2026-54799 | A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.20), SICORE Base system (All versions < V26.20.0). The affected application contains a vulnerability in its firmware update mechanism's signature validation process. This could allow an attacker to install malicious firmware, leading to persistent code execution and system compromise. |
| CVE-2026-59837 | A stack-based buffer overflow vulnerability in Fortinet FortiOS 7.4.0 through 7.4.1, FortiOS 7.2 all versions, FortiPAM 1.8.0 through 1.8.2, FortiPAM 1.7 all versions, FortiPAM 1.6 all versions, FortiPAM 1.5 all versions, FortiPAM 1.4 all versions, FortiPAM 1.3 all versions, FortiPAM 1.2 all versions, FortiPAM 1.1 all versions, FortiPAM 1.0 all versions, FortiProxy 7.4.0 through 7.4.13, FortiProxy 7.2 all versions may allow a privileged authenticated attacker who can bypass stack protection and ASLR to execute arbitrary code or commands via crafted HTTP requests. |
| CVE-2026-62239 | FlashAttention through 2.8.3.post1, fixed in commit 0816ef1, contains a symlink attack vulnerability in the download_and_copy() function within hopper/setup.py that extracts NVIDIA toolchain archives without validating symlinks or filtering tar members. A local attacker can pre-plant a symlink in the predictable cache directory to redirect extracted binaries to an attacker-chosen location, enabling arbitrary file write with victim privileges during build time. |
| CVE-2026-50678 | Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to disclose information locally. |
| CVE-2025-11977 | The Happyforms – Form Builder for WordPress: Drag & Drop Contact Forms, Surveys, Payments & Multipurpose Forms plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.26.12 via the happyforms_get_form_partial() function. This makes it possible for authenticated attackers, with Administrator-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included. |
| CVE-2026-49804 | Heap-based buffer overflow in Windows USB Video Driver allows an unauthorized attacker to elevate privileges with a physical attack. |
| CVE-2026-13080 | The WPFunnels – Funnel Builder for WooCommerce with Checkout & One Click Upsell plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.12.7 via the 'logKey' parameter parameter. This makes it possible for authenticated attackers, with administrator-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included. |
| CVE-2026-11426 | The UnderConstructionPage PRO plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 5.76. This is due to the plugin accepting arbitrary local file paths in the template_thumbnail parameter and copying their contents into a publicly accessible uploads file. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read arbitrary files on the server, which can contain sensitive information. |
| CVE-2026-57391 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tangible Loops & Logic tangible-loops-and-logic allows Stored XSS.This issue affects Loops & Logic: from n/a through <= 4.2.3. |
| CVE-2026-10106 | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to verify that the channel referenced in an action cookie matches the channel of the target post, which allows an authenticated user without access to a private channel to trigger interactive post actions on posts in that channel via a cookie obtained from any accessible channel.. Mattermost Advisory ID: MMSA-2026-00690 |
| CVE-2026-1365 | Insertion of sensitive information into sent data vulnerability in Sayax Energy Technologies Inc. OSOS allows Authentication Bypass. This issue affects OSOS: through 09072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-57390 | Missing Authorization vulnerability in EDGARROJAS Extra Product Options Builder for WooCommerce additional-product-fields-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Extra Product Options Builder for WooCommerce: from n/a through <= 1.2.167. |
| CVE-2026-49876 | Authenticated SSRF in Gravitino JobManager allows server-side HTTP requests to internal network and cloud metadata endpoints via unvalidated job template URIs. A vulnerability in Apache Gravitino. This issue affects Apache Gravitino: from 1.0.0 through 1.2.1. Users are recommended to upgrade to version 1.3.0, which fixes the issue. |
| CVE-2026-8996 | The Backup and Staging by WP Time Capsule plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.22.26 via the download_recent_decrypted_file_wptc. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract download the most recently admin-decrypted SQL database backup, which typically contains password hashes, user credentials, and other sensitive site configuration data stored in the 'recent_decrypted_file' option. Exploitation requires that an administrator has previously performed a decrypt action, causing the decrypted SQL backup file to exist in the plugin's upload directory; without this prior admin action, there is no file to serve. |
| CVE- | |

| | |
|---|---|
| 2026-57976 | Null pointer dereference in Active Directory Domain Services allows an authorized attacker to deny service over a network. |
| CVE-2026-57364 | Improper Validation of Specified Quantity in Input vulnerability in WPDeveloper Better Payment – Instant Payments, Donations, Fundraising with Subscriptions & More better-payment allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Better Payment – Instant Payments, Donations, Fundraising with Subscriptions & More: from n/a through <= 2.2.0. |
| CVE-2026-55003 | Use of uninitialized resource in Windows RDP allows an unauthorized attacker to disclose information over a network. |
| CVE-2026-57365 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hitesh Chandwani reCAPTCHA (v2 & v3) for Asgaros Forum recaptcha-for-asgaros-forum allows DOM-Based XSS.This issue affects reCAPTCHA (v2 & v3) for Asgaros Forum: from n/a through <= 1.1.0. |
| CVE-2026-57392 | Missing Authorization vulnerability in Themefic Tourfic tourfic allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tourfic: from n/a through <= 2.22.5. |
| CVE-2026-57783 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in merkulove Speaker speaker allows Stored XSS.This issue affects Speaker: from n/a through <= 4.1.13. |
| CVE-2026-57979 | Out-of-bounds read in Windows RDP allows an unauthorized attacker to disclose information over a network. |
| CVE-2026-57780 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Plugin Envision Envision Page Builder envision-page-builder allows DOM-Based XSS.This issue affects Envision Page Builder: from n/a through <= 0.22. |
| CVE-2026-58279 | Missing authorization in Azure CycleCloud allows an authorized attacker to elevate privileges over a network. |
| CVE-2026-6850 | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to validate the length and content of message attachment field values, which allows an authenticated attacker to cause a denial of service for all users in a channel via a post containing a specially crafted payload that triggers catastrophic backtracking in the client-side markdown parser.. Mattermost Advisory ID: MMSA-2026-00658 |
| CVE-2026-56460 | HCL DevOps Deploy / HCL Launch could disclose sensitive configurations and secrets to authenticated users in API responses that could be used in further attacks against the system. |
| CVE-2026-54798 | A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.20), SICORE Base system (All versions < V26.20.0). The affected application includes a debugging interface that is accessible through HTTP endpoints. This could allow an authenticated attacker to disrupt the system by crashing the web process causing denial of service conditions. |
| CVE-2026-12428 | The Blocks for ACF Fields plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the get_all_values() function in the /wp-json/acf-field-blocks/v1/values REST endpoint in versions up to, and including, 1.6.2. The permission_callback only verifies the generic publish_posts capability and the handler passes a user-supplied id parameter directly to get_field_objects() without verifying that the requesting user is authorized to read the target object. This makes it possible for authenticated attackers, with Author-level access and above, to read ACF field values from arbitrary posts (including private posts, drafts, posts by other users, and other ACF-supported objects) that they should not have access to. |
| CVE-2026-56185 | Improper authentication in Windows Admin Center allows an authorized attacker to disclose information over a network. |
| CVE-2026-6280 | Exposure of sensitive information due to incompatible policies vulnerability in NOMYSOFT Informatics Education and Consulting Inc. Nomysem allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Nomysem: through 08072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-57259 | The input file does not need to be strictly in a structurally valid PDF format. Instead, after reviewing the content, the original document disguised as a PDF will be sent to the parser. Malicious documents will construct malicious external entities that, through the protocol, point to local paths, thereby allowing access to any local files within the user's permission range. |
| CVE-2026-15073 | The KiviCare – Clinic & Patient Management System (EHR) plugin for WordPress is vulnerable to generic SQL Injection via the 'orderby' parameter in all versions up to, and including, 4.5.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Doctor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires a KiviCare Doctor, Receptionist, or Clinic Admin role at minimum, as the vulnerable REST endpoint is restricted to authenticated users with custom plugin-level access. |
| CVE-2026-57393 | Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in EDGARROJAS WooCommerce PDF Invoice Builder woo-pdf-invoice-builder allows Retrieve Embedded Sensitive Data.This issue affects WooCommerce PDF Invoice Builder: from n/a through <= 2.0.8. |
| CVE-2026-15072 | The KiviCare – Clinic & Patient Management System (EHR) plugin for WordPress is vulnerable to generic SQL Injection via the 'orderby' parameter in all versions up to, and including, 4.5.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with doctor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This requires that the attacker hold at minimum a KiviCare Doctor-level account, or a Receptionist or Clinic Admin role that grants the doctor_session_list capability. |
| CVE-2026-60095 | Vinchin Backup & Recovery through 9.0.0.86562 contains a stack buffer overflow vulnerability in the ModuleHandShake function of the agentlink_server service that allows unauthenticated remote attackers to overwrite the saved return address by supplying an oversized _listen_uuid field that is measured via strlen() and copied without bounds checking into a fixed-length stack buffer using strcpy(). Attackers can send a crafted request with a malicious _listen_uuid value to corrupt the stack and achieve process crash or potential control flow hijack without requiring authentication. |
| CVE- | |

| | |
|---|---|
| 2026-60001 | sshd in OpenSSH before 10.4 does not always honor the minimum authentication delay. |
| CVE-2026-57375 | Missing Authorization vulnerability in FluxBuilder MStore API mstore-api allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MStore API: from n/a through <= 4.18.4. |
| CVE-2026-60094 | Vinchin Backup & Recovery through 9.0.0.86562 contains a heap buffer overflow vulnerability that allows unauthenticated remote attackers to cause process crash or memory corruption by sending a malformed TCP packet with an unchecked body_len field to the agentlink_server service. Attackers can craft a malicious packet that passes an attacker-controlled length directly to recv(), triggering a heap overflow of up to approximately 4 GiB and resulting in process crash or potential memory corruption. |
| CVE-2026-13262 | The Majestic Support – The Leading-Edge Help Desk & Customer Support Plugin plugin for WordPress is vulnerable to generic SQL Injection via the 'val' parameter in all versions up to, and including, 1.1.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires a valid 'get-smart-reply' nonce, which any Subscriber-level user can obtain by creating a ticket via the public frontend and visiting the resulting ticket detail page, making this effectively exploitable by any authenticated user. |
| CVE-2026-50445 | Buffer over-read in Windows RDP allows an unauthorized attacker to disclose information over a network. |
| CVE-2026-57377 | Missing Authorization vulnerability in WPXPO WowAddons product-addons allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WowAddons: from n/a through <= 1.6.8. |
| CVE-2026-57693 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Spacetime Ad Inserter ad-inserter allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ad Inserter: from n/a through <= 2.8.11. |
| CVE-2026-12270 | The Everest Forms WordPress plugin before 3.5.0 does not correctly restrict access to several REST API endpoints belonging to its onboarding assistant: the capability check is only applied when an attacker-controllable request header holds a specific value, so it can be bypassed by omitting or changing that header. This makes it possible for unauthenticated attackers to read onboarding status information, modify the related Everest Forms WordPress plugin before 3.5.0 options, and trigger an email from the site to an arbitrary address. |
| CVE-2026-57395 | Missing Authorization vulnerability in Themefic Tourfic tourfic allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tourfic: from n/a through <= 2.22.5. |
| CVE-2026-13011 | The ERP: Complete HR, Accounting & CRM Suite with Recruitment and WooCommerce CRM Support plugin for WordPress is vulnerable to generic SQL Injection via the 'orderby' parameter in all versions up to, and including, 1.17.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with custom-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires the erp_list_employee capability, which is granted to HR Manager-level users and above within the WP ERP plugin. |
| CVE-2026-57414 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in QuantumCloud ChatBot for eCommerce – WoowBot woowbot-woocommerce-chatbot allows Stored XSS.This issue affects ChatBot for eCommerce – WoowBot: from n/a through <= 4.6.1. |
| CVE-2026-57711 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PSM Plugins SupportCandy supportcandy allows Stored XSS.This issue affects SupportCandy: from n/a through <= 3.4.8. |
| CVE-2026-57418 | Missing Authorization vulnerability in BoldGrid Client Invoicing by Sprout Invoices sprout-invoices allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Client Invoicing by Sprout Invoices: from n/a through <= 20.8.13. |
| CVE-2026-59262 | AFFiNE's histories GraphQL field fails to validate Doc.Read permission before exposing document edit history, allowing authenticated workspace members to retrieve restricted content timelines. Attackers can supply arbitrary document GUIDs to access full edit histories including user names, emails, and timestamps of private pages they lack access to. |
| CVE-2026-50376 | Use of uninitialized resource in Windows RDP allows an unauthorized attacker to disclose information over a network. |
| CVE-2026-57698 | Authentication Bypass Using an Alternate Path or Channel vulnerability in VillaTheme Abandoned Cart Recovery for WooCommerce woo-abandoned-cart-recovery allows Authentication Abuse.This issue affects Abandoned Cart Recovery for WooCommerce: from n/a through <= 1.1.12. |
| CVE-2026-59820 | LiteLLM is a proxy server (AI Gateway) to call LLM APIs in OpenAI (or native) format. Prior to 1.83.7-stable, LiteLLM Skills archive extraction did not sufficiently validate file paths from uploaded skill ZIP archives, allowing an authenticated user with access to LiteLLM LLM API routes or a key whose allowed_routes includes /v1/skills, anthropic_routes, or llm_api_routes to upload a crafted skill archive containing path traversal entries that could be written outside the intended extraction or staging directory. This issue is fixed in version 1.83.7-stable. |
| CVE-2026-57419 | Missing Authorization vulnerability in Fahad Mahmood Stock Locations for WooCommerce stock-locations-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Stock Locations for WooCommerce: from n/a through <= 3.1.8. |
| CVE-2026-57420 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Netrr Author Box WP Lens author-box-for-divi allows Stored XSS.This issue affects Author Box WP Lens: from n/a through <= 2.1.5. |
| CVE-2026-59896 | Hono is a Web application framework that provides support for any JavaScript runtime. From 4.11.8 before 4.12.27, hono/jsx did not isolate context values per request during server-side rendering, allowing createContext, useContext, jsxRenderer, or useRequestContext data from a different in-flight request to be used after an await in an async component. This issue is fixed in version 4.12.27. |
| CVE-2026- | Authorization Bypass Through User-Controlled Key vulnerability in Themeum Tutor LMS tutor allows Exploiting Incorrectly Configured Access Control Security |

| | |
|---|---|
| 57694 | Levels.This issue affects Tutor LMS: from n/a through <= 3.9.13. |
| CVE-2026-50366 | Null pointer dereference in Active Directory Domain Services allows an authorized attacker to deny service over a network. |
| CVE-2026-15154 | A flaw was found in `guardrails-detectors`, a component of Red Hat OpenShift AI. This vulnerability, known as Regular Expression Denial of Service (ReDoS), allows a remote attacker to provide specially crafted regular expressions to the public detection API. This can cause catastrophic backtracking, leading to a worker process consuming 100% CPU indefinitely and resulting in a denial of service for the entire guardrails-mediated LLM pipeline. |
| CVE-2026-57812 | Missing Authorization vulnerability in NSquared Simply Schedule Appointments simply-schedule-appointments allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Simply Schedule Appointments: from n/a through <= 1.6.12.4. |
| CVE-2026-57424 | Missing Authorization vulnerability in knitpay Razorpay Payment Links for WooCommerce rzp-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Razorpay Payment Links for WooCommerce: from n/a through <= 2.1.4. |
| CVE-2026-58254 | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.3 and 2.12.8, message trace destination checks were applied to ordinary client connections but not consistently to messages arriving through leafnode connections, allowing a leafnode operator to send trace events to subjects that would not otherwise be permitted and to use trace-only behavior to prevent normal delivery or storage of affected messages. This issue is fixed in versions 2.14.3 and 2.12.8. |
| CVE-2026-58252 | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.0, 2.12.7, and 2.11.16, an authenticated user could receive messages on denied subjects when a wildcard subscription overlapped with a configured wildcard deny rule but was not a subset of it, and queue subscriptions could also affect delivery to legitimate queue consumers. This issue is fixed in versions 2.14.0, 2.12.7, and 2.11.16. |
| CVE-2026-57412 | Missing Authorization vulnerability in Codemenschen Gift Vouchers gift-voucher allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Gift Vouchers: from n/a through <= 4.6.9. |
| CVE-2026-57408 | Missing Authorization vulnerability in peachpayments Peach Payments Gateway wc-peach-payments-gateway allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Peach Payments Gateway: from n/a through <= 4.0.2. |
| CVE-2026-35211 | OpenCTI is an open source platform for managing cyber threat intelligence knowledge and observables. Prior to 7.260401.0, the OpenCTI GraphQL API exposes a script filter operator in its FilterOperator enum that allows any authenticated user with the KNOWLEDGE capability to pass user-supplied Elasticsearch Painless script values directly into search queries without validation or sanitization, allowing computationally expensive scripts to consume cluster CPU resources and degrade or deny service for all users. This issue is fixed in version 7.260401.0. |
| CVE-2026-54777 | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, CoreWCF NetNamedPipe transport accepts attachment to a pre-existing named pipe instance, allowing local interception of NetNamedPipe traffic when an attacker races NamedPipeListener startup between shared memory GUID publication and service named pipe creation. This issue is fixed in versions 1.8.1 and 1.9.1. |
| CVE-2026-58251 | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.0, 2.12.7, and 2.11.16, an authenticated user with subscription deny permissions could bypass a plain subject deny rule by using a queue subscription, because queue-specific deny evaluation could override the plain subject deny result when the queue name itself was not denied. This issue is fixed in versions 2.14.0, 2.12.7, and 2.11.16. |
| CVE-2026-54775 | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, a CoreWCF service listening on a Kafka topic stops processing new records from that topic when KafkaTransportPump receives a null-value tombstone record, causing a persistent endpoint denial of service for attackers with produce permission. This issue is fixed in versions 1.8.1 and 1.9.1. |
| CVE-2026-56220 | Capgo before 12.128.2 contains an authorization bypass vulnerability in the public.manifest INSERT policy that allows read-only org members to insert OTA manifest rows. Attackers with read-only org access can inject malicious manifest entries with arbitrary s3_path values that are served to devices via the unauthenticated /updates endpoint, enabling OTA metadata poisoning and potential malicious asset delivery. |
| CVE-2026-12274 | The Tutor LMS WordPress plugin before 3.9.13 does not verify that the requesting user is allowed to edit a target post before overwriting it in one of its content-builder save handlers, authorizing the request only against an unrelated identifier, allowing authenticated users with instructor-level access to overwrite and take over any post or page on the site, including those owned by administrators. |
| CVE-2026-59888 | jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.15.0 until 2.18.8, 2.21.4, and 3.1.4, Java Records using a PropertyNamingStrategy can bypass @JsonIgnore because POJOPropertiesCollector._removeUnwantedIgnorals() records an ignored component under its original implicit name before _renameUsing() applies the naming strategy, allowing the renamed JSON key to be assigned to the Record constructor parameter. This issue is fixed in versions 2.18.8, 2.21.4, and 3.1.4. |
| CVE-2026-56273 | Flowise before 3.1.0 contains a path traversal vulnerability in Faiss and SimpleStore vector store implementations that accept unsanitized basePath parameters from authenticated users. Attackers with valid API tokens can write vector store data to arbitrary filesystem locations, potentially enabling code execution or data exfiltration. |
| CVE-2026-15109 | Uninitialized Use in ANGLE in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-57400 | Missing Authorization vulnerability in WP Swings Event Tickets Manager for WooCommerce event-tickets-manager-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Event Tickets Manager for WooCommerce: from n/a through <= 1.5.5. |
| CVE-2026-57406 | Missing Authorization vulnerability in Roxnor FundEngine wp-fundraising-donation allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects FundEngine: from n/a through <= 1.7.6. |
| CVE-2026-48492 | Snipe-IT is an IT asset/license management system. Prior to version 8.6.1, the GET /api/v1/{object}/selectlist API endpoint is missing an authorization check. Any user who can log into Snipe-IT - regardless of permissions - can retrieve a paginated list of all user accounts using only their web session cookie. No API token or elevated permissions are required. This exposes usernames, display names, employee numbers, and user IDs for every active account in the system if FMCS is not enabled, and within the company they belong to if FMCS is enabled. Version 8.6.1 contains a patch. |
| CVE-2026- | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdesk Flexible Refund and Return Order for WooCommerce flexible-refund-and-return-order-for-woocommerce allows Stored XSS.This issue affects Flexible Refund and Return Order for WooCommerce: from n/a through <= |

| | |
|---|---|
| 57402 | 1.0.51. |
| CVE-2026-59818 | etcd is a distributed key-value store for the data of a distributed system. Prior to 3.5.32 and 3.6.13, when etcd is configured with --listen-client-http-urls to split HTTP and gRPC client endpoints onto separate listeners, the --client-crl-file Certificate Revocation List is not enforced on the gRPC listener, allowing a client with a revoked certificate to authenticate successfully over gRPC. This issue is fixed in versions 3.5.32 and 3.6.13. |
| CVE-2026-58494 | Wasmtime is a runtime for WebAssembly. Prior to 24.0.11, 36.0.12, 45.0.3, and 46.0.1, wasmtime-wasi hard-link creation and renaming check directory permissions but not matching FilePerms on source and destination preopens, allowing a WASI guest with a read-only source file capability to overwrite host files exposed as FilePerms::READ through wasip1, wasip2, or wasip3 filesystem interfaces. This issue is fixed in versions 24.0.11, 36.0.12, 45.0.3, and 46.0.1. |
| CVE-2026-56401 | Wazuh wazuh-modulesd before 5.0.0-beta3 contains a null pointer dereference vulnerability in inventory_sync FlatBuffer DataValue handling. An enrolled agent can send a verifier-valid DataValue message omitting the optional id field, causing wazuh-modulesd to crash when dereferencing data->id()->string_view() without null validation, resulting in denial of service. |
| CVE-2026-58191 | Appium is a cross-platform automation framework for all kinds of apps, built on top of the W3C WebDriver protocol. Prior to 10.7.0, Appium's base-driver unconditionally mounts the /test/guinea-pig, /test/guinea-pig-scrollable, and /test/guinea-pig-app-banner routes, and compileLodashTemplate reflects the throwError query parameter, comments POST field, and User-Agent request header into HTML without escaping, allowing reflected cross-site scripting and arbitrary JavaScript execution on the server origin. This issue is fixed in version 10.7.0. |
| CVE-2026-57404 | Missing Authorization vulnerability in magepeopleteam Booking and Rental Manager booking-and-rental-manager-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Booking and Rental Manager: from n/a through <= 2.6.9. |
| CVE-2026-59805 | Gumroad before 2026.07.06.2 contains a broken access control vulnerability in the PurchasesController that allows authenticated sellers to manipulate purchase access for other sellers' products by sending PUT requests to the revoke_access and undo_revoke_access actions without seller ownership validation. Attackers can modify the is_access_revoked status on arbitrary purchases to unauthorized revoke or restore buyer access to products they do not own. |
| CVE-2026-57019 | An Improper Validation of Specified Quantity in Input vulnerability in the Packet Forwarding Engine (pfe) of Juniper Networks Junos OS on MX Series allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). When a specific packet is received from device in the same broadcast domain, an affected system calculates the packet size incorrectly. This causes further packet processing to fail, which triggers an FPC major error, resulting in a FPC reset impacting traffic until the FPC has automatically recovered. Affected scenarios are: MAP-T, or non-IP traffic encapsulated in IP (e.g. MPLS over GRE). When this issue happens the following logs can be observed: fpc<#> CMError: /fpc/0/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_LI_INT_REG_UNROLL_TAIL_LENGTH_OVF (0x2205eb), scope: pfe, category: functional, severity: major, module: MQSS(0), type: LI: Unroll TAIL length overflow, oc_category: default fpc<#> Performing action reset-fru for error /fpc/0/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_LI_INT_REG_UNROLL_TAIL_LENGTH_OVF (0x2205eb) in module: MQSS(0) with scope: pfe category: functional level: major, oc_category: default This issue affects Junos OS on MX Series: * all versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S7, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S4, * 25.2 versions before 25.2R2. |
| CVE-2026-57032 | An Improper Handling of Undefined Parameters vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on EX Series devices allows an authenticated attacker with low privileges to cause a Denial-of-Service (DoS). If an attempt is made to subscribe to an unsupported telemetry sensor path on EX2300, EX3400, EX4000, EX4100 and EX4400 via gRPC, this causes the FPC to crash. This leads to a complete service outage until the module has automatically restarted. The following log message can be seen when this issue happens: agentd[<PID>]: AGENTD_RESOURCE_NOT_FOUND: No resource name found for <sensor> This issue affects Junos OS on EX2300, EX3400, EX4000, EX4100 and EX4400 devices: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S5, * 24.4 versions before 24.4R2. |
| CVE-2026-57217 | RabbitMQ is a messaging and streaming broker. Prior to 3.13.15, 4.0.21, 4.1.11, and 4.2.6, RabbitMQ topic authorization can allow restricted topic writes and binds during metadata-store failures because topic-permission lookup errors from Khepri can collapse to undefined, which the internal backend treats as allow. This issue is fixed in versions 3.13.15, 4.0.21, 4.1.11, and 4.2.6. |
| CVE-2026-56312 | Capgo before 12.128.2 contains an improper validation vulnerability in the accept_invitation endpoint that creates user accounts before captcha validation is enforced. Attackers can bypass captcha protection by sending POST requests with invalid captcha tokens to create unwanted accounts and burn invite links. |
| CVE-2026-57027 | A Missing Release of Memory after Effective Lifetime vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on specific EX Series devices allows an unauthenticated adjacent attacker to cause a Denial-of-Service (DoS).When sFlow is configured in a Virtual Chassis (VC) scenario with EX4100 Series or EX4400 Series devices, multicast traffic which is received on one VC member and sent out on another member leads to a memory leak and ultimately an FPC crash and restart. The leak can be monitored by watching the continuous increase of the buffer values in the output of: user@host> show chassis fpc This issue affects Junos OS on EX4100 Series and EX4400: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S7, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2. |
| CVE-2026-33803 | An Improper Restriction of Communication Channel to Intended Endpoints vulnerability in Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause a limited information disclosure and availability impact to the device. Due to a wrong initialization, a process which should only be able to communicate internally within the device can be reached over the network via an open port. This leads to a device being inadvertently exposed and increased CPU cycles spent processing ingress packets. This issue affects Junos OS Evolved: * all versions before 23.2R2-S7-EVO, * 23.4 versions before 23.4R2-S8-EVO, * 24.2 versions before 24.2R2-S5-EVO, * 24.4 versions before 24.4R2-S4-EVO, * 25.2 versions before 25.2R2-S1-EVO, * 25.4 versions before 25.4R1-S2-EVO. |
| CVE-2026-59198 | Pillow is a Python imaging library. From 5.2.0 until 12.3.0, Pillow's TGA RLE encoder reads past its packed row buffer when saving a mode 1 image with TGA RLE compression, allowing adjacent process heap bytes to be copied into the generated TGA file. This issue is fixed in version 12.3.0. |
| CVE-2026-55469 | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, an authenticated user with import and assets.update permissions can place a path traversal string in an asset image field through CSV import and then trigger image deletion, allowing deletion of arbitrary files accessible to the server process. This issue is fixed in version 8.6.2. |
| CVE-2026-49488 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache OpenMeetings. This issue affects Apache OpenMeetings: from 5.0.0 before 9.1.0. An attacker with moderator rights in any room can read arbitrary files accessible to the OS account running the OM server, including credentials and secrets, via a crafted download request. Users are recommended to upgrade to version 9.1.0, which fixes the issue. |
| CVE-2026-0282 | A file deletion vulnerability in Palo Alto Networks PAN-OS® software enables an unauthenticated attacker with network access to the management web interface to delete files from a temporary directory. The security risk posed by this issue is minimized by restricting access to the management web interface to only trusted internal IP addresses according to our recommended best practice deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series). Cloud NGFW and Prisma® Access are not impacted by this vulnerability. |
| CVE-2026-57211 | RabbitMQ is a messaging and streaming broker. Prior to 4.1.11 and 4.2.6 on Windows, the RabbitMQ management plugin static file handler rabbit_mgmt_wm_static can pass URL-encoded backslashes to erl_prim_loader:read_file_info before path validation when multiple management extension plugins are enabled, causing outbound DNS and SMB requests to attacker-controlled UNC paths. This issue is fixed in versions 4.1.11 and 4.2.6. |

| | |
|---|---|
| CVE-2026-56335 | Capgo before 12.128.2 contains an authorization bypass vulnerability where write-scoped API keys can directly mutate protected channel configuration fields through PostgREST by exploiting a null authentication check in the immutability trigger. Attackers with write API keys can modify sensitive channel attributes such as public, allow_emulator, and security-related flags outside intended application routes. |
| CVE-2026-57020 | An Improper Check for Unusual or Exceptional Conditions vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on QFX10000 Series allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). On all QFX10000 platforms in an EVPN-VxLAN scenario, if an attacker sends IPv6 multicast traffic and these packets reach the non-IRB interface of a spine switch it floods the packet to other spines and all Ethernet Segment Identifier (ESI) leaf switches. This flooding causes the packet to be forwarded in a endless loop, which can lead to saturation of the involved links and in turn impact to legitimate traffic. This issue affects Junos OS on QFX10000 Series: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S4. This issue does not affect Junos version after 24.4 as the QFX10000 Series devices are not supported on newer versions anymore. |
| CVE-2026-57218 | RabbitMQ is a messaging and streaming broker. Prior to 4.2.6, RabbitMQ AMQP 0-9-1 allows an existing consumer to keep receiving messages after OAuth token expiry or connection.update_secret refresh to reduced scopes because existing consumers are not canceled or reauthorized at delivery time after the channel user state changes. This issue is fixed in version 4.2.6. |
| CVE-2026-15104 | The BetterDocs – AI Documentation, Knowledge Base, Docs, Wikis, FAQ with Chatbot plugin for WordPress is vulnerable to generic SQL Injection via the 'lang' parameter in all versions up to, and including, 4.6.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with custom-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires a supported multilingual plugin (WPML, Polylang, qTranslate, Weglot, or TranslatePress) to be active on the site, as the vulnerable code path is gated by Helper::is_multilingual_active(). |
| CVE-2026-59149 | Mockoon provides way to design and run mock APIs. Prior to 9.7.0, a FILE response whose filePath embeds request data is confined by getSafeFilePath in packages/commons-server/src/libs/server/server.ts with resolvedPath.startsWith(staticBaseDir). That prefix test has no path-separator boundary, so a ../-escaped path whose absolute form string-prefixes the base directory passes, allowing an unauthenticated client to read files from sibling paths outside the served directory through HTTP sendFile, WebSocket, or callbacks. This issue is fixed in version 9.7.0. |
| CVE-2026-13242 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Drupal Geolocation Field allows SQL Injection. This issue affects Geolocation Field versions: from 0.0.0 to 3.15.0. |
| CVE-2026-53961 | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, the AWS SES bounce webhook at POST /webhooks/aws verified that SNS messages were signed by Amazon but did not bind them to trusted TopicArn values, allowing any AWS account holder to publish validly signed forged Bounce notifications that revoke a targeted user email. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5. |
| CVE-2026-13241 | Missing Authorization vulnerability in Drupal Paragraphs allows Forceful Browsing. This issue affects Paragraphs versions: from 0.0.0 to 1.21.0. |
| CVE-2026-13240 | Missing Authorization vulnerability in Drupal Paragraphs allows Forceful Browsing. This issue affects Paragraphs versions: from 0.0.0 to 1.21.0. |
| CVE-2026-33801 | An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent, unauthenticated attacker sending a specific BGP update over an established BGP session to cause a Denial-of-Service (DoS). Upon receipt of a specifically malformed non-inet/inet6 unicast BGP update, an RPD crash and restart is triggered, which will cause a complete service outage until routing has reconverged. The rpd crash occurs before the update can be readvertised, so there is no downstream propagation. This issue affects: * Junos OS versions 25.2 before 25.2R2; * Junos OS Evolved versions 25.2 before 25.2R2-EVO. This issue doesn't affect Junos OS versions before 25.2R1 nor Junos OS Evolved versions before 25.2R1-EVO. |
| CVE-2026-13239 | Missing Authorization vulnerability in Drupal WissKI allows Forceful Browsing. This issue affects WissKI versions: from 0.0.0 to 4.2.0. |
| CVE-2026-46413 | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, regular users could route direct S3 multipart uploads through ExternalUploadManager into the admin backup store. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5. |
| CVE-2026-54468 | Dell Unisphere for PowerMax, version(s) 10.3.0.5 and prior, contain(s) a path traversal vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability to read arbitrary files. |
| CVE-2026-33800 | An Unchecked Input for Loop Condition vulnerability in the Packet Forwarding Engine (pfe) of Juniper Networks Junos OS on MX Series allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS).Micro-BFD session flaps generate respective up/down events which are queued by PFEMAN for processing. Especially in a Virtual-Chassis (VC) scenario with locality-bias configured, processing takes a significant amount of time for each event. If these sessions keep flapping, new events are constantly added, and in turn PFEMAN never completes processing these events. This results in the PFEMAN watchdog timer expiring, which causes the FPC to crash and restart, representing a complete service outage. This issue only affects MX series FPCs up to and including MPC9. It does not affect MPC10/11, LC4800/9600 and MX304. This issue affects Junos OS on MX Series: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S3, * 25.2 versions before 25.2R2. |
| CVE-2026-49799 | Uncontrolled resource consumption in Windows Local Security Authority Subsystem Service (LSASS) allows an authorized attacker to deny service over a network. |
| CVE-2026-58408 | ChurchCRM is an open-source church management system. Prior to version 7.4.0, a low-privileged user can bypass the /admin/export UI and exfiltrate the entire member directory. The POST /CSVCreateFile.php endpoint generates and streams a CSV containing the full Personally Identifiable Information (PII) of every Person/Family record in the database, without performing any feature-level or object-level authorization check beyond the coarse "has any admin permission" gate inherited from the legacy page bootstrap. In other words, any single non-admin permission flag is enough to reach the CSV bulk-export endpoint, even though such users should not have data export rights. The export script is missing a dedicated isAdmin() (or a new bExportData) authorization check of its own. This issue has been fixed in version 7.4.0. |
| CVE-2026-54108 | External control of file name or path in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network. |
| CVE-2026-34348 | Protection mechanism failure in Windows Event Logging Service allows an authorized attacker to disclose information over a network. |

| | |
|---|---|
| CVE-2026-57157 | FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.28.0, FreeRDP server implementations with the MS-RDPECAM camera device enumerator channel enabled scan attacker-supplied DeviceName and VirtualChannelName fields for a NUL terminator in channels/rdpecam/server/camera_device_enumerator_main.c and then dereference once past the scan bound, allowing a malicious RDP client to trigger a 1- to 2-byte out-of-bounds heap read. This issue is fixed in version 3.28.0. |
| CVE-2026-11944 | openSIS Classic 9.3 contains an authenticated path traversal vulnerability in the legacy messaging sent-mail attachment download functionality that allows an authenticated attacker to read arbitrary files on the server via crafted path traversal sequences. |
| CVE-2026-40009 | Improper Privilege Management, Improper Access Control vulnerability in Apache IoTDB. Authenticated users can escalate to full tree-path access by renaming themselves to __internal_auditor. This issue affects Apache IoTDB: from 2.0.8 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue. |
| CVE-2026-59207 | n8n is an open source workflow automation platform. Prior to 2.27.4 and 2.28.1, the AI Agents feature did not enforce the Allowed HTTP Request Domains restriction configured on credentials when an MCP tool was pointed at an arbitrary URL, allowing a member-level user with use-only access to a shared credential to send its secret to an external server they control. This issue is fixed in versions 2.27.4 and 2.28.1. |
| CVE-2026-47282 | Insufficiently protected credentials in GitHub Copilot and Visual Studio Code allows an unauthorized attacker to disclose information over a network. |
| CVE-2026-59523 | Missing Authorization vulnerability in NSquared Simply Schedule Appointments simply-schedule-appointments allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Simply Schedule Appointments: from n/a through <= 1.6.11.11. |
| CVE-2026-58478 | Sustainable Irrigation Platform (SIP) through version 5.2.16 contains a server-side request forgery (SSRF) vulnerability that allows unauthenticated attackers to make the device issue arbitrary HTTP requests by supplying a malicious callback URL when the optional Node-RED plugin is installed. Attackers can exploit the lack of destination validation and the default passphrase 'opendoor' to send blind HTTP requests to arbitrary internal or external hosts not otherwise directly accessible. |
| CVE-2026-15192 | A vulnerability has been found in mettle sendportal up to 3.0.1. This issue affects the function sendgrid/postmark/postal/mailjet of the component APIv1 Webhooks. The manipulation leads to missing authentication. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-51598 | An input validation vulnerability in the RTSP service of MERCURY MIPC252W IP Camera v1.0.5 Build 230306 Rel.79931n) allows an unauthenticated, network-adjacent attacker to cause a denial of service via a crafted DESCRIBE request with a malformed URL in the request line. |
| CVE-2026-55843 | Snipe-IT is an IT asset/license management system. Prior to 8.6.0, UsersController::update() passes a missing permission request field through NormalizePermissionsPayloadAction and PreserveUnauthorizedPrivilegedPermissionsAction in a way that can overwrite a target user’s permissions with a sparse result, allowing an administrator updating another administrator, or a user with users.edit updating a regular account, to remove the target’s administrative or granular permissions. This issue is fixed in version 8.6.0. |
| CVE-2026-62147 | The Tempo Operator's gateway component failed to consistently apply namespace-scoped redaction on some query API response paths when query RBAC was enabled, allowing an authenticated user to read span attributes belonging to other tenants' namespaces. |
| CVE-2026-13010 | The JoomSport – for Sports: Team & League, Football, Hockey & more plugin for WordPress is vulnerable to time-based SQL Injection via 'event' Shortcode Attribute in all versions up to, and including, 5.7.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The shortcode can be embedded in posts or pages by Contributor-level users, making this exploitable by any authenticated user with at least that role. |
| CVE-2026-55474 | Snipe-IT is an IT asset/license management system. Prior to 8.5.0, ActionlogController::displaySig concatenates the route filename parameter into a private upload-directory path without sanitization, allowing an authenticated attacker to traverse outside the intended directory and read arbitrary files accessible to the web server process. This issue is fixed in version 8.5.0. |
| CVE-2026-59209 | n8n is an open source workflow automation platform. Prior to 1.123.61, 2.27.4, and, 2.28.1, an authenticated member with use-only editor access to a shared workflow could read credential-populated headers exposed via the $request object inside an HTTP Request node's pagination expression and exfiltrate the secret through item data. This issue is fixed in versions 1.123.61, 2.27.4, and 2.28.1. |
| CVE-2026-15287 | The rtMedia for WordPress, BuddyPress and bbPress plugin for WordPress is vulnerable to time-based SQL Injection via the order_by parameter in all versions up to, and including, 4.6.18 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. |
| CVE-2026-59220 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.2 before 0.10.0, the SKILL_MENTION_RE and strip_re regular expressions in backend/open_webui/utils/middleware.py parsed <$skillId\|label> skill mentions with overlapping quantifiers, allowing an authenticated chat message containing <$ without a closing > to trigger quadratic backtracking and block the asyncio event loop. This issue is fixed in version 0.10.0. |
| CVE-2026-59222 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.7.0 before 0.10.0, GET /api/v1/channels//members returned full UserModelResponse objects for channel members, including settings.ui.toolServers[].key and webhook configuration, allowing a normal channel participant to retrieve other users’ sensitive settings. This issue is fixed in version 0.10.0. |
| CVE-2026-61455 | Grav before 2.0.1 contains a decompression bomb vulnerability in ZipArchiver::extract() that lacks limits on uncompressed size, file count, and nesting depth. Attackers can supply a crafted ZIP archive that expands to fill available disk space, causing denial of service by exhausting storage resources. |
| CVE-2026-61450 | Grav before 2.0.2 contains a Twig sandbox bypass that allows a page author (any admin.pages user, or anyone able to write to user/pages) to exfiltrate configuration secrets. Although the sandbox replaces the 'config' variable with a redacted facade and strips Config::get/toArray from the method allowlist, the raw container remains accessible via the allow-listed grav.offsetGet('config'), which returns the real Config object. Allow-listed object-dumping filters (json_encode, print_r, yaml_encode) then serialize that object at the PHP level without invoking the sandbox method gate, exposing the full config tree including plugin secrets such as SMTP credentials, API keys, and plugin DB credentials. This is an incomplete fix for GHSA-j274-39qw-32c9. |
| CVE-2026-59853 | SiYuan is an open-source personal knowledge management system. Prior to 3.7.1, the /api/storage/getCriteria endpoint returns saved search criteria from data/storage/criteria.json without the publish-access filtering used by sibling storage endpoints, allowing a publish-mode Reader to read private document paths, notebook, document, and block IDs, and search and replace keywords for unpublished documents. This issue is fixed in versions 3.7.1. |
| | |

| | |
|---|---|
| CVE-2026-61441 | PraisonAI Platform (praisonai-platform) before 0.1.9 improperly authorizes deletion of issue dependencies. The DELETE dependency route accepts either endpoint of a dependency edge and checks delete permission only against the caller-selected URL issue. A workspace member who cannot delete a dependency through an owner-created issue endpoint (which returns 403) can delete the same dependency edge by targeting a related member-owned issue endpoint, because permission is validated against the member-owned issue's owner. This allows members to bypass owner/admin authorization and remove owner-created issue dependencies. |
| CVE-2026-57413 | Server-Side Request Forgery (SSRF) vulnerability in bdthemes Instant Image Generator ai-image allows Server Side Request Forgery.This issue affects Instant Image Generator: from n/a through <= 2.1.4. |
| CVE-2025-14785 | The Website Builder by SeedProd - Theme Builder, Landing Page Builder, Coming Soon Page, Maintenance Mode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `seedprodnestedmenuwidget` shortcode in all versions up to, and including, 6.20.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-3907 | The Hostel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wphostel-book' shortcode in all versions up to and including 1.1.7. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes. Specifically, the second shortcode attribute (used as button text) is passed to the `$text` variable without sanitization at line 79 and then output directly into an HTML `value` attribute at line 91 without `esc_attr()` or any other escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-6742 | The Advanced iFrame plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'additional' parameter in all versions up to, and including, 2026.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-10660 | The Bluetooth BAP Broadcast Assistant GATT client in subsys/bluetooth/audio/bap_broadcast_assistant.c reassembled remote Broadcast Receive State data into a single file-static net_buf_simple (att_buf, BT_ATT_MAX_ATTRIBUTE_LEN = 512 bytes) shared by all connection instances, while the BUSY flag, long-read handle, and reset/offset state were per-connection. When the device acts as a Broadcast Assistant connected to multiple Scan Delegator peripherals, notification and long-read callbacks from different connections interleave on the shared buffer: the append in notify_handler (net_buf_simple_add_mem at the not-busy branch) performs no tailroom check, so receive-state notifications from two or more delegators accumulate on the same 512-byte buffer and, with a sufficiently large configured ATT MTU (BT_L2CAP_TX_MTU up to 2000) and two-to-three concurrent connections, write past the buffer into adjacent .bss (net_buf_simple_add only asserts in debug builds). Even below the overflow threshold, one connection's net_buf_simple_reset zeroes the shared length while another connection's reassembly and GATT read offset are in flight, mixing one peer's data into another's parse. A malicious or compromised Scan Delegator (or two colluding peers) over BLE can trigger this, causing out-of-bounds writes (memory corruption / denial of service) and cross-connection data corruption. The fix moves the buffer into the per-connection instance struct so each connection reassembles into its own buffer. Affects Zephyr releases shipping the Broadcast Assistant with the shared buffer, including v4.4.0 and earlier. |
| CVE-2026-12924 | The Eventin – Event Calendar, Event Registration, Tickets & Booking (AI Powered) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'etn_faq_content' parameter in all versions up to, and including, 4.1.15 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-4018 | TOCTOU Race Condition in specific trace commands of the TraceEvent() system call could allow an attacker with local access and with the PROCMGR_AID_TRACE ability, to cause information disclosure, data tampering or a crash of the QNX Neutrino kernel. |
| CVE-2026-15296 | The affiliate-toolkit – WP Affiliate Plugin with Amazon plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'atkp_product' shortcode in all versions up to, and including, 3.7.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is a bypass to CVE-2024-10227. |
| CVE-2026-62644 | In Roundcube Webmail before 1.6.17 and 1.7.x before 1.7.2, the password plugin of the Roundcube Webmail was subject to username spoofing via session data, which could lead to account takeover. |
| CVE-2026-8649 | Improper Neutralization of Special Elements in Data Query Logic vulnerability in Progress MOVEit Transfer (Custom Reports modules). This issue affects MOVEit Transfer: before 2025.0.7, from 2025.1.0 before 2025.1.3. |
| CVE-2026-15292 | The Sudoku Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'background' parameter in the 'sudoku-sc' shortcode in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-12123 | The All-in-One Video Gallery plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 4.8.5 via the 'vdl' parameter. This makes it possible for authenticated attackers, with subscriber-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. A Subscriber-level attacker can plant an internal or loopback URL in the `mp4` post meta of a newly created `aiovg_videos` post via XML-RPC `wp.newPost`, then trigger the unauthenticated `?vdl=<post_id>` endpoint to force the server to fetch that URL and stream the full response body back to the requester. |
| CVE-2026-6740 | The Nexter Blocks – Gutenberg Blocks, Page Builder & AI Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'commentIcon' parameter in all versions up to, and including, 4.7.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-12988 | The WP 2FA WordPress plugin before 3.1.1.2 does not verify that the email address supplied during two-factor authentication setup belongs to the user, allowing an attacker who has obtained a user's credentials to redirect the setup verification code to an attacker-controlled email address and take over the account. |
| CVE-2026-15299 | The Animation Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'weather_style' and 'move_direction' parameters of the Weather widget in all versions up to, and including, 2.6.3. This is due to insufficient output escaping in the Weather widget's render() function at widgets/weather.php:1246, where both settings values are placed into an HTML class attribute without esc_attr(). Elementor does not server-side validate widget SELECT control values against allowed options on save, so an authenticated attacker with Contributor-level access or above can submit a crafted save_builder AJAX request storing arbitrary values in the _elementor_data post meta. The stored payload renders unescaped on every frontend visit to the affected page (the Weather widget requires an OpenWeatherMap API key to reach the vulnerable output, which is the normal operational state for sites using this widget). |
| CVE-2026- | The Ultimate Post plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'moreResultsText' block attribute of the ultimate-post/advanced-search block in versions up to and including 5.0.31. This is due to insufficient input sanitization and output escaping in the Advanced_Search::content() render callback: the attribute value is filtered with wp_kses(), which strips disallowed HTML tags but does NOT escape HTML special characters such as double quotes in plain text, |

| | |
|---|---|
| 13253 | and the result is then concatenated directly into the data-viewmoretext HTML attribute without esc_attr(). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-57097 | Untrusted search path in Microsoft XML allows an unauthorized attacker to bypass a security feature with a physical attack. |
| CVE-2026-6910 | The Bookero.pl – system rezerwacji online plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `bookero_products` shortcode's `hide_products` (and `filter_products`) attributes in versions up to and including 2.2. This is due to insufficient input sanitization and output escaping in the `bookero_products()` function — the raw attribute value is concatenated directly into an inline `<script>` block without any escaping. This makes it possible for authenticated attackers with contributor-level access and above to inject arbitrary web scripts into pages that will execute whenever a user accesses the injected page. |
| CVE-2026-11390 | The News Kit Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Site Logo Title and Single Author Box Widgets in all versions up to, and including, 1.4.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires an attacker to intercept and modify the elementor_ajax AJAX save request in order to bypass the client-side SELECT control restrictions and submit arbitrary tag-name values. |
| CVE-2026-7640 | The WP Customer Area plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'type' attribute of the `customer-area-protected-content` shortcode in all versions up to, and including, 8.3.5. This is due to insufficient input sanitization and output escaping on the shortcode attribute. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-55000 | Use after free in Windows USB Print Driver allows an unauthorized attacker to elevate privileges with a physical attack. |
| CVE-2026-11321 | The DataInjection plugin for GLPI 2.15.6 (GLPI 11 builds) concatenates user-supplied CSV field values directly into SQL queries during CSV import, without parameterization or escaping, resulting in authenticated SQL injection. An authenticated user with access to the Data injection feature can embed SQL expressions such as SLEEP() in a mapped field (for example Serial Number) to manipulate the generated query and extract database information via time-based blind injection. |
| CVE-2026-53987 | The Tag plugin for GLPI 11 before 2.14.4 stores the tag name without HTML sanitization and renders it into the Kanban badge markup via PluginTagTag::preKanbanContent() without output escaping, resulting in stored cross-site scripting. An authenticated user with TAG MANAGEMENT create or update rights can set a tag name containing HTML, which then executes in the browser of any user who opens the Kanban view of a ticket, problem, change, or project the tag is attached to. |
| CVE-2026-13710 | The Jeg Kit for Elementor – Powerful Addons for Elementor, Widgets & Templates for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Image Box widget's 'sg_body_description' parameter in versions up to, and including, 3.2.6. This is due to insufficient input sanitization and output escaping on the description attribute in the render_body() method of the Image_Box_View class — every other attribute used by the method is wrapped in esc_attr(), but the description value is concatenated directly into HTML body context. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-5743 | The SimpLy Gallery Block & Lightbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via block attributes in all versions up to, and including, 3.3.3.2. This is due to insufficient input sanitization and output escaping on the sliderMaxHeight block attribute in the pgc_sgb_render_callback() function. The vulnerability exists because the pgc_sgb_sanitize_custom_css() function uses a flawed regex pattern that only removes event handlers with quoted values (e.g., onfocus="alert()") but fails to catch unquoted event handlers (e.g., onfocus=alert(document.cookie)), allowing the malicious code to bypass sanitization. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages via block attributes that will execute whenever a user accesses an injected page. |
| CVE-2025-13968 | The Starboard Suite Reservation Calendars plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcode attributes in the [starboard-suite-lightbox] shortcode in all versions up to, and including, 3.1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-13247 | The Logo Slider – Logo Carousel, Client Logo Slider & Brand Showcase for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'lgx_tooltip_position' parameter in all versions up to, and including, 5.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-3251 | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Webremium Istanbul Web Design Mezunum Satiyorum allows Stored XSS. This issue affects Mezunum Satiyorum: from 1.2.504 through 10072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-56778 | n8n before 2.25.7 and 2.26.x before 2.26.2 contains an authorization bypass in the Public API execution retry endpoint, which authorizes access using the workflow:read scope instead of workflow:execute. An authenticated user with read-only access to a shared workflow can use the Public API to retry executions of that workflow, bypassing the intended permission boundary between read and execute access. This affects instances where workflows are shared with other users or across projects. |
| CVE-2026-15096 | The Themify Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Map Module 'b_width_map' Field in all versions up to, and including, 7.7.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-15097 | The Themify Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'height_slider' Slider Module Field in all versions up to, and including, 7.7.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-15301 | The BuddyHolis TableSearch plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘placeholder’ parameter in all versions up to, and including, 1.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-15284 | The King Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'form_page_id' parameter in versions up to, and including, 51.1.62 This is due to insufficient input sanitization in the add_to_submissions() function, which applies sanitize_text_field() (which preserves double-quote characters) before storing the value in post meta, combined with missing output escaping in the king_addons_submissions_custom_column_content() function, which concatenates the stored value into an HTML href attribute via admin_url() without wrapping the result in esc_url(). This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026- | The Block, Suspend, Report for BuddyPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link' parameter in versions up to and including 3.6.4. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with subscriber-level access and above |

| | |
|---|---|
| 4653 | to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-15285 | The Plus Addons for Elementor plugin for WordPress was vulnerable to Authenticated (Contributor+) Stored Cross-Site Scripting via the Button widget's `custom_attributes` setting in versions up to and including 6.4.11. The `render` function in `modules/widgets/tp_button.php` passed the raw `custom_attributes` string through `tp_senitize_js_input()`. This filter is bypassable. The issue is patched in version 6.4.12. |
| CVE-2026-55370 | Logto is the modern, open-source auth infrastructure for SaaS and AI apps. Prior to 1.41.0, Logto's existing TOTP verification accepted a successfully used TOTP code again while the code remained inside the RFC 6238 acceptance window because the verifier used otplib's stateless check with window = 1 and did not persist or compare the accepted TOTP time-step counter. An attacker who has the victim's first factor and captures a live TOTP value can replay that value to satisfy MFA during the same acceptance window. This issue is fixed in version 1.41.0. |
| CVE-2026-1382 | The fresh Podcaster plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'freshpodcaster' shortcode in all versions up to, and including, 1.0.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-6459 | The Essential Addons for Elementor – Popular Elementor Templates & Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Event Calendar widget in all versions up to, and including, 6.6.2 due to insufficient input sanitization and output escaping on event titles sourced from The Events Calendar. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-15010 | The bbp Style Pack plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 6.4.5 via the Topic Form Additional Fields feature. This is due to insufficient input sanitization in bsp_topic_fields_form_save() (which writes $_POST['bsp_topic_fields_label{n}'] directly to post meta via update_post_meta() with no filtering) and missing output escaping in bsp_topic_content_append_topic_fields() (which concatenates the stored meta value into an HTML  and echoes it via apply_filters/echo without esc_html()). This makes it possible for authenticated attackers, with Subscriber-level access and above (who have bbPress topic-creation privileges), to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page, including unauthenticated visitors. |
| CVE-2026-12170 | The AcyMailing – An Ultimate Newsletter Plugin and Marketing Automation Solution for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'alignment' attribute in all versions up to, and including, 10.10.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-12126 | The WCFM Marketplace – Multivendor Marketplace for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Attachment 'post_title' in all versions up to, and including, 3.7.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Vendor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. An attacker can plant the payload by uploading a media attachment with a crafted title via the WordPress REST API (/wp-json/wp/v2/media), without ever invoking the AJAX endpoint themselves, as the unescaped title is later emitted inside DataTables JSON and inserted as innerHTML upon any privileged user loading the media dashboard. |
| CVE-2026-10570 | The Sympl Repeater for ACF and Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via ACF repeater field values in all versions up to, and including, 2.3. This is due to insufficient input sanitization and output escaping in the symp_arfe_replace_content() function, which uses str_replace() to substitute raw ACF field values (retrieved via get_field()) directly into Elementor-rendered HTML without any escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-13771 | The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'color' Shortcode Attribute in all versions up to, and including, 5.113.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-14343 | The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'note_before' and 'note_after' Shortcode Attributes in all versions up to, and including, 3.3.61 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Because wp_kses_post filters post content on save for users without unfiltered_html, only kses-allowed tag and attribute payloads that survive save-time filtering will reach the unescaped sink; however, the sink itself remains unsafe and such payloads can still execute in the browser when a user renders the shortcode. |
| CVE-2026-12536 | The Avada (Fusion) Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘Module Title’ parameter in all versions up to, and including, 3.15.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-56329 | Capgo before 12.128.2 contains a cross-tenant preview namespace collision vulnerability caused by non-bijective decoding of double underscores to dots in preview hostname parsing. Attackers can register app IDs with underscores that collide with other tenants' dotted app IDs, causing preview misrouting and denial of preview access for victim applications. |
| CVE-2026-50374 | Use after free in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges with a physical attack. |
| CVE-2026-15501 | A security vulnerability has been detected in AstrBotDevs AstrBot up to 4.25.2. Affected by this issue is the function ToolsRoute.test_mcp_connection of the file astrbot/dashboard/routes/tools.py of the component MCP Test Endpoint. The manipulation of the argument mcp_server_config.url leads to server-side request forgery. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15502 | A vulnerability was detected in AojiaoZero Antaris 1.0. This affects the function _rewardPurchase of the file /ipn.php of the component PayPal IPN Payment Handler. The manipulation of the argument item_number results in sql injection. The attack may be performed from remote. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15702 | A security vulnerability has been detected in tamagui up to 2.3.0. This affects the function updateConfig of the file code/core/web/src/config.ts. Such manipulation leads to improperly controlled modification of object prototype attributes. The attack may be performed from remote. Upgrading to version 2.3.1 is able to mitigate this issue. The name of the patch is e46af9879b7627934ea4d6d6e46e65cea53abb3d. The affected component should be upgraded. |
| CVE-2026-50375 | Heap-based buffer overflow in Windows DirectX allows an authorized attacker to elevate privileges locally. |
| CVE-2026-15496 | A vulnerability was found in SonicCloudOrg sonic-agent up to 2.7.2. The impacted element is the function evalIsFailed of the file sonic-agent/src/main/java/org/cloud/sonic/agent/tests/script/GroovyScriptImpl.java of the component Groovy Script Handler. The manipulation results in os command injection. The attack can be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer. |
| CVE- | |

| | |
|---|---|
| 2026-15507 | A vulnerability was detected in coollabsio Coolify up to 4.1.1. The impacted element is an unknown function of the file /app/Policies/ of the component Policy Handler. Performing a manipulation results in missing authorization. Remote exploitation of the attack is possible. The exploit is now public and may be used. |
| CVE-2026-15508 | A flaw has been found in Helicone ai-gateway up to 0.2.0-beta.30. This affects the function build_target_url of the file ai-gateway/src/dispatcher/service.rs of the component AWS Metadata Service. Executing a manipulation of the argument extracted_path_and_query can lead to server-side request forgery. The attack can be executed remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15697 | A vulnerability was found in svgdotjs svg.js up to 3.2.5. This affects the function EventTarget.on of the file svgdotjs/svg.js of the component npm Package API. Performing a manipulation results in improperly controlled modification of object prototype attributes. The attack may be initiated remotely. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-15536 | A vulnerability was identified in itsourcecode Hospital Management System 1.0. This affects an unknown part of the file /patviewprescription.php. The manipulation of the argument delid leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. |
| CVE-2026-15535 | A vulnerability was determined in AkariAsai self-rag up to 1fcdc420e48f50a7d7ab1ece5494221b93252e99. Affected by this issue is the function Indexer.deserialize_from of the file retrieval_lm/src/index.py of the component retrieval_lm. Executing a manipulation of the argument index_meta.faiss can lead to deserialization. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-15698 | A vulnerability was determined in kofrasa mingo up to 7.2.1. This impacts the function update/updateOne/updateMany of the component Update API. Executing a manipulation of the argument Set can lead to improperly controlled modification of object prototype attributes. The attack may be launched remotely. Upgrading to version 7.2.2 will fix this issue. This patch is called fadc398251792c2ba441cbc539f359fc7943c0c2. It is recommended to upgrade the affected component. |
| CVE-2026-15620 | A security vulnerability has been detected in mosaxiv clawlet up to 0.2.10. This affects the function tools.webFetch of the file tools/tool_web_fetch.go. Such manipulation leads to server-side request forgery. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The reported GitHub issue was closed with the label "not planned". |
| CVE-2026-15619 | A weakness has been identified in mosaxiv clawlet up to 0.2.10. The impacted element is the function web_fetch of the file tools/tool_web_fetch.go of the component IPv4 Handler. This manipulation of the argument url causes server-side request forgery. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The reported GitHub issue was closed with the label "not planned". |
| CVE-2026-15618 | A security flaw has been discovered in mosaxiv clawlet up to 0.2.10. The affected element is the function guardExecCommand of the file tools/tool_exec.go of the component exec Safety Guard. The manipulation results in protection mechanism failure. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The reported GitHub issue was closed with the label "not planned". |
| CVE-2026-15033 | A flaw has been found in christopherthielen check-peer-dependencies up to 4.3.4. Affected by this vulnerability is the function shelljs.exec of the file dist/packageUtils.js of the component peerDependencies. This manipulation causes os command injection. The attack may be initiated remotely. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-15529 | A vulnerability was detected in yzhao062 pyod 3.5.0/3.5.1/3.5.2. Affected is the function pyod.utils.persistence.load of the file pyod/utils/persistence.py. Performing a manipulation of the argument path results in deserialization. The attack can be initiated remotely. The pull request to fix this issue requires some minor changes. |
| CVE-2026-15538 | A weakness has been identified in primefaces primereact up to 10.9.8. This issue affects the function ObjectUtils.mutateFieldData of the component API. This manipulation of the argument Field causes improperly controlled modification of object prototype attributes. The attack is possible to be carried out remotely. The project was informed of the problem early through an issue report but has not responded yet. This vulnerability only affects products that are no longer supported by the maintainer. |
| CVE-2026-15525 | A vulnerability was detected in kLOsk adloop up to 0.9.0. This vulnerability affects the function _validate_urls of the file src/adloop/ads/write.py. Performing a manipulation of the argument final_url results in server-side request forgery. The attack may be initiated remotely. The exploit is now public and may be used. Upgrading to version 0.10.0 is able to resolve this issue. The patch is named 217399723e3a2fb39389e5355d49ed80aaf9ea7c. Upgrading the affected component is advised. |
| CVE-2026-15626 | A vulnerability was determined in nextlevelbuilder GoClaw 3.13.3-beta.3. This affects the function writeFile of the file internal/providers/acp/tool_bridge.go of the component ACP ToolBridge Workspace Handler. This manipulation causes path traversal. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. |
| CVE-2026-15523 | A weakness has been identified in CodeAstro Simple Online Leave Management System 1.0. Affected by this issue is some unknown functionality of the file /SimpleOnlineLeave/admin/dashboard.php. This manipulation of the argument Name causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. |
| CVE-2026-15044 | A flaw was found in the TrustyAI Service Operator. When deploying services like gorch or NemoGuardrails, if a specific security setting is not enabled, these services can expose their communication channels without requiring users to prove their identity. This allows any other program within the cluster to access the AI guardrails and orchestrator without proper authorization. An attacker could exploit this to gain unauthorized access to sensitive information and potentially make limited changes to the AI models. |
| CVE-2026-55668 | File Browser provides a web file managing interface. Prior to 2.63.16, ScopedFs validates the nearest existing ancestor of a dangling symlink as in scope and then follows the symlink during file creation, allowing an authenticated user with Create and Modify permissions to create attacker-controlled files outside the user's scope. This issue is fixed in version 2.63.16. |
| CVE-2026-15628 | A security flaw has been discovered in zhayujie chatgpt-on-wechat CowAgent up to 2.1.1. This issue affects the function Vision._download_to_data_url of the file agent/tools/vision/vision.py of the component Vision Tool. Performing a manipulation of the argument image results in server-side request forgery. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 2.1.2 is capable of addressing this issue. The patch is named e85290cddcbb5ffc9c235927f4c92e5b4c3ec264. The affected component should be upgraded. |
| CVE-2026-15063 | A flaw was found in the gorch service template, which is part of the trustyai-service-operator. Even when authentication is enabled, the gorch service exposes unproxied orchestrator and detector metrics ports. This allows any pod on the cluster network to directly access these ports, bypassing the kube-rbac-proxy and its authentication mechanisms. This could lead to unauthorized access to the orchestrator and detector metrics. |
| CVE-2026-15513 | A security flaw has been discovered in Wavlink WL-NU516U1 260515. This affects the function wlink_uci_set_value of the file /cgi-bin/adm.cgi. Performing a manipulation of the argument lan_ip results in os command injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. You should upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product. |
| CVE- | A vulnerability was identified in pig-mesh Pig up to 3.9.2. Affected by this issue is some unknown functionality of the file \pig-master\pig-visual\pig-codegen\src\main\java\com\pig4cloud\pig\codegen\service\impl\GeneratorServiceImpl.java of the component pig-codegen. Such manipulation leads to code |

| | |
|---|---|
| 2026-15512 | 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. |
| CVE-2026-15510 | A vulnerability was found in Leantime up to 3.8.0. Affected is the function Setting::saveSetting of the component API. The manipulation results in improper authorization. The attack may be performed from remote. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15509 | A vulnerability has been found in Leantime up to 3.8.0. This impacts the function editUser/addUser of the component JSON-RPC Endpoint. The manipulation of the argument role leads to improper authorization. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15699 | A vulnerability was identified in spencermountain compromise up to 14.15.1. Affected is the function nlp.extend of the file src/API/extend.js of the component Public Root API. The manipulation of the argument plugin leads to improperly controlled modification of object prototype attributes. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The identifier of the patch is b4644ab7179700df0607521f61c1ee9b5f78d89d. Applying a patch is the recommended action to fix this issue. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product. |
| CVE-2026-15473 | A vulnerability was identified in Eleveo Call Recording Software 9.7.0. This issue affects some unknown processing of the file /callrec/restoreCallAction.do of the component Recorded Calls Page. The manipulation leads to improper authorization. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15332 | A security flaw has been discovered in zhayujie CowAgent up to 2.1.0. The impacted element is an unknown function of the file channel/channel.py of the component Message Endpoint. The manipulation results in missing authorization. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-56877 | The SCORM lab launch endpoint in Skillable (scorm.skillable.com) through 2026-07-13 does not validate the client-supplied userId parameter against the authenticated SCORM session token. An authenticated user can substitute arbitrary userId values to bypass per-user lab launch rate limits and consume other users' lab allocations, resulting in denial of service against targeted users' lab and exam access. Skillable was formerly named Learn on Demand Systems. |
| CVE-2026-39179 | A SQL injection vulnerability in SOGo before 5.12.7 allows authenticated users to execute arbitrary SQL statements via the newPassword parameter in the password change functionality. |
| CVE-2026-15105 | A flaw has been found in davenardella snap7 up to 1.4.3. This affects the function TS7Worker::PerformFunctionRead of the file src/core/s7_server.cpp of the component ReadVar Request Handler. This manipulation causes deserialization. The attack requires access to the local network. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-15598 | A weakness has been identified in antv layout 2.0.0. This impacts the function setNestedValue in the library lib/util/object.js. Executing a manipulation of the argument path can lead to improperly controlled modification of object prototype attributes. The attack can be launched remotely. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-15138 | A security vulnerability has been detected in tumf mcp-text-editor up to 1.0.2. This issue affects the function _validate_file_path of the file mcp_text_editor/text_editor.py. Such manipulation of the argument file_path leads to path traversal. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor closed the GitHub issue for this vulnerability without any explanation. |
| CVE-2026-15672 | A vulnerability was determined in itsourcecode Electronic Judging System 1.0. Impacted is an unknown function of the file /intrams/admin/add_judges.php. This manipulation of the argument fname causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. |
| CVE-2026-15374 | A flaw has been found in Eleveo Call Recording Software 9.7.0. This affects an unknown function of the file /callrec/roleAddAction.do of the component Group Interface. Executing a manipulation can lead to improper authorization. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15195 | A weakness has been identified in apidevtools json-schema-ref-parser up to 15.3.5. This impacts the function Refs.set/Pointer.set in the library lib/pointer.ts. Executing a manipulation can lead to improperly controlled modification of object prototype attributes. The attack can be launched remotely. Upgrading to version 15.3.6 will fix this issue. This patch is called a786bc6afc3674f650496472ee93d5cf74c4bd84. It is suggested to upgrade the affected component. |
| CVE-2026-15373 | A vulnerability was detected in Eleveo Call Recording Software 9.7.0. The impacted element is an unknown function of the file /callrec/userAddAction.do. Performing a manipulation of the argument role results in improper authorization. It is possible to initiate the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15376 | A vulnerability was found in Eleveo Call Recording Software 9.7.0. Affected is an unknown function of the file /callrec/statisticReportAction.do. The manipulation results in improper authorization. The attack can be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15559 | A vulnerability was detected in CodeAstro Simple Online Leave Management System 1.0. This affects an unknown part of the file /SimpleOnlineLeave/admin/accept.php of the component POST Handler. Performing a manipulation of the argument appid results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used. |
| CVE-2026-15558 | A security vulnerability has been detected in CodeAstro Simple Online Leave Management System 1.0. Affected by this issue is some unknown functionality of the file /SimpleOnlineLeave/admin/deletemp.php. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. |
| CVE-2026-15186 | A vulnerability was identified in macrozheng mall up to 1.0.3. This impacts an unknown function of the file /returnApply/create of the component Portal Endpoint. The manipulation of the argument orderId leads to improper control of resource identifiers. The attack can be initiated remotely. The exploit is publicly available and might be used. The vendor deleted the GitHub issue for this vulnerability without any explanation. |
| CVE-2026-15191 | A flaw has been found in mettle sendportal up to 3.0.1. This vulnerability affects unknown code of the file vendor/mettle/sendportal-core/src/Http/Requests/CampaignStoreRequest.php of the component Campaign Creation Endpoint. Executing a manipulation can lead to authorization bypass. The attack can be executed remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-15188 | A weakness has been identified in manjurulhoque django-job-portal up to dfa352f305bba44445ac5dc12e9b2a98c9dcd71f. Affected by this vulnerability is the function EditEmployeeProfileAPIView of the file accounts/api/views.py of the component Employee Dashboard Endpoint. This manipulation of the argument role causes improper access controls. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet. |

| | |
|---|---|
| CVE-2026-15189 | A security vulnerability has been detected in aerostackdev aerostack-mcp up to 6315dfde7df0a15aaf743f88d91347115e09ba23. Affected by this issue is the function upload_media of the component mcp-whatsapp. Such manipulation of the argument media_url leads to server-side request forgery. The attack may be launched remotely. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-39178 | A SQL injection vulnerability in SOGo before 5.12.7 allows authenticated users to execute arbitrary SQL statements via the search parameter of the allContactSearch endpoint. |
| CVE-2026-15624 | A vulnerability has been found in nextlevelbuilder GoClaw 3.13.3-beta.3. Affected by this vulnerability is the function bytePlusDownloadVideo of the file internal/tools/create_video_byteplus.go of the component invoke Endpoint. The manipulation of the argument output.video_url leads to server-side request forgery. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. |
| CVE-2026-15318 | A weakness has been identified in Sipeed PicoClaw up to 0.2.9. Affected by this issue is some unknown functionality of the file pkg/channels/mqtt/mqtt.go of the component MQTT Channel Handler. This manipulation of the argument client_id causes incorrect authorization. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. The reported GitHub issue was closed automatically due to inactivity. |
| CVE-2026-15547 | A weakness has been identified in Shibby Tomato up to 1.28.0000. This affects the function sub_2D048 of the component CIFS Mount Handler. Executing a manipulation of the argument cifs1/cifs2 can lead to os command injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. This project is superseded by FreshTomato. |
| CVE-2026-15487 | A vulnerability was found in TRENDnet TEW-821DAP 1.11B03. This impacts the function sub_41FBD0 of the file /goform/system_ntp of the component Firmware Update Handler. Performing a manipulation of the argument Hostname results in os command injection. The attack may be initiated remotely. The vendor explains: "We are unable to confirm the existence of the vulnerabilities for (...) TEW-821DAP (v1.0R) as these items have been EOL. " This vulnerability only affects products that are no longer supported by the maintainer. |
| CVE-2026-15486 | A vulnerability has been found in TRENDnet TEW-821DAP 1.11B03. This affects the function sub_42026C of the file /goform/tools_ddns of the component Firmware Update Handler. Such manipulation of the argument hostname/username/password leads to os command injection. The attack can be launched remotely. The vendor explains: "We are unable to confirm the existence of the vulnerabilities for (...) TEW-821DAP (v1.0R) as these items have been EOL. " This vulnerability only affects products that are no longer supported by the maintainer. |
| CVE-2026-15485 | A flaw has been found in TRENDnet TEW-821DAP 1.11B03. The impacted element is the function sub_43F2C4 of the file /goform/tools_nslookup of the component DNS Lookup Handler. This manipulation of the argument nslookup_target/dns_server causes os command injection. The attack can be initiated remotely. The vendor explains: "We are unable to confirm the existence of the vulnerabilities for (...) TEW-821DAP (v1.0R) as these items have been EOL. " This vulnerability only affects products that are no longer supported by the maintainer. |
| CVE-2026-15499 | A security flaw has been discovered in AstrBotDevs AstrBot up to 4.25.2. Affected is the function FutureTaskTool.call of the file astrbot/core/tools/cron_tools.py of the component Scheduled Task Handler. Performing a manipulation of the argument payload["note"] results in improper authorization. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15500 | A weakness has been identified in AstrBotDevs AstrBot up to 4.25.2. Affected by this vulnerability is the function get_online_plugins of the file astrbot/dashboard/routes/plugin.py of the component market_list Endpoint. Executing a manipulation of the argument custom_registry can lead to server-side request forgery. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15546 | A security flaw has been discovered in Shibby Tomato up to 1.28.0000. Affected by this issue is the function sub_2D568 of the component start_jffs2. Performing a manipulation of the argument jffs2_exec results in os command injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. This project is superseded by FreshTomato. |
| CVE-2026-14250 | The Themehunk Login Registration plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 1.0.2. This is due to the handle_frontend_register() function in the unauthenticated /thlogin/v1/register REST endpoint accepting a user-controlled 'role' parameter and validating it only against get_editable_roles() — which returns every defined editable site role, including 'editor' — before passing it to wp_insert_user(). This makes it possible for unauthenticated attackers, when public user registration is enabled, to create new accounts with the editor role. |
| CVE-2026-15668 | A vulnerability has been found in louisho5 picobot up to 0.2.0. This vulnerability affects the function WebTool.Execute of the file internal/agent/tools/web.go of the component web Tool. The manipulation of the argument url leads to server-side request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-15495 | A vulnerability has been found in SonicCloudOrg sonic-agent up to 2.7.2. The affected element is an unknown function of the file AndroidWSServer.java of the component Android WebSocket Server. The manipulation of the argument path leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer. |
| CVE-2026-15478 | A flaw has been found in IceHRM up to 35.0.1. This impacts an unknown function of the file core/src/Reports/User/Reports/EmployeeAttendanceReport.php of the component UserReport Endpoint. Executing a manipulation of the argument employeeList can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-15629 | A weakness has been identified in louisho5 picobot up to 0.2.0. Impacted is the function CreateSkill/GetSkill of the file internal/agent/tools/filesystem.go of the component Workspace Handler. Executing a manipulation can lead to link following. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-15477 | A vulnerability was detected in Bahmni bahmnicore up to 0.93. This affects the function additionalParams of the file /openmrs/ws/rest/v1/bahmnicore/sql of the component Search Endpoint. Performing a manipulation of the argument test results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used. Upgrading to version 0.93.1, 1.0.1, 1.1.1, 1.2.1, 1.3.1 and 2.0.1 mitigates this issue. Upgrading the affected component is recommended. |
| CVE-2026-15317 | A security flaw has been discovered in Sipeed PicoClaw up to 0.2.9. Affected by this vulnerability is the function WebFetchTool.Execute of the file pkg/tools/integration/web.go of the component Guarded Web Fetch Flow. The manipulation results in server-side request forgery. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. The reported GitHub issue was closed automatically due to inactivity. |
| CVE-2026-15625 | A vulnerability was found in nextlevelbuilder GoClaw 3.11.3. Affected by this issue is the function ExecApprovalManager.CheckCommand of the file internal/tools/exec_approval.go. The manipulation results in incomplete blacklist. The attack can be executed remotely. The exploit has been made public and could be used. |
| CVE-2026-0515 | Insufficient Parameter Validation in the SchedGet() system call could allow an attacker with local access to cause a crash of the QNX Neutrino kernel. |

| | |
|---|---|
| CVE-2026-50420 | Out-of-bounds read in Windows HTTP.sys allows an unauthorized attacker to disclose information locally. |
| CVE-2026-49807 | Exposure of sensitive information to an unauthorized actor in Windows DirectX allows an unauthorized attacker to disclose information locally. |
| CVE-2026-56459 | HCL DevOps Deploy / HCL Launch is susceptible to sensitive information disclosure.  The application stores potentially sensitive information in log files that could be read by a local user. |
| CVE-2026-39245 | decompress before 4.2.2 contains an improper path containment check that enables directory traversal and arbitrary file write. The safeMakeDir function (index.js line 29) and the extraction path validation (index.js line 106) use String.indexOf() to verify the resolved path is within the output directory: realDestinationDir.indexOf(realOutputPath) !== 0. This check is flawed because it does not enforce a path separator boundary. For example, "/tmp/app_config".indexOf("/tmp/app") returns 0, incorrectly passing the check even though /tmp/app_config is outside /tmp/app. Combined with the unvalidated symlink creation in the same package, an attacker can write arbitrary files to directories adjacent to the extraction target. This is a bypass of the fix for CVE-2020-12265. The correct check requires appending a path separator: realParentPath.indexOf(realOutputPath + path.sep) !== 0. |
| CVE-2026-50294 | Exposure of sensitive system information to an unauthorized control sphere in Windows Kernel allows an unauthorized attacker to disclose information locally. |
| CVE-2026-54778 | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, CoreWCF UnixDomainSocket POSIX peer identity resolution uses non-reentrant getpwuid and getgrgid calls, allowing concurrent connections to attribute one connection's identity to another or crash the host process under contention. This issue is fixed in versions 1.8.1 and 1.9.1. |
| CVE-2026-50453 | Out-of-bounds read in Windows USB Audio Class driver (usbaudio.sys) allows an unauthorized attacker to disclose information with a physical attack. |
| CVE-2026-57258 | The PRC file header parsing logic trusts the constructed file structure description information, assumes that the underlying array contains elements and reads them, leading to out-of-bounds reads and application crashes. |
| CVE-2026-58475 | Sustainable Irrigation Platform (SIP) through version 5.2.16 contains a stored cross-site scripting vulnerability that allows unauthenticated attackers to inject arbitrary JavaScript by supplying malicious script payloads within program names submitted via HTTP requests. Attackers can exploit the lack of output encoding on rendered program names to execute arbitrary JavaScript in the browsers of any users viewing the affected page, with exploitation facilitated by the absence of a required passphrase or the default passphrase 'opendoor'. |
| CVE-2026-11798 | The Social Share, Social Login and Social Comments Plugin – Super Socializer plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'heateor_mastodon_share' parameter in all versions up to, and including, 7.14.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. |
| CVE-2026-57241 | The application opens the PDF, and JavaScript performs operations on the page and the document, causing the page-related objects within the application to lose synchronization; however, the renderer still trusts the outdated page count, and eventually the application crashes due to out-of-bounds access. |
| CVE-2026-57243 | During the process of page opening and form formatting, a JavaScript reentrancy results in an inconsistent document status. Subsequently, with outdated page information, the application attempts to access invalid addresses, causing the application to crash. |
| CVE-2026-57253 | An abnormal image object causes the renderer to enter the wrong processing branch. When converting the scan lines, an invalid image buffer pointer is used, resulting in the application crashing. |
| CVE-2026-57255 | The application opens a PDF containing an abnormal color space whose attributes reference a valid but semantically malformed function. The function's output is not validated; when subsequently read, it produces an illegal pointer that accesses an out-of-bounds region, crashing the application. |
| CVE-2026-8310 | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Webbeyaz Web Design Mediküm Web allows Reflected XSS. This issue affects Mediküm Web: through 08072026. NOTE: The vendor was contacted and it was learned that the product is not supported. |
| CVE-2026-57829 | The Joomla extension Helix Ultimate is vulnerable to an unauthenticated stored XSS. |
| CVE-2026-57257 | During the PRC parsing stage, there is a lack of boundary verification for the PRC entity index, which leads to an out-of-bounds read of the entity array. As a result, the application crashes. |
| CVE-2026-54988 | Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally. |
| CVE-2026-44767 | setThemeRoot() failed to enforce the sap-allowed-theme-origins allowlist. An attacker-controlled absolute cross-origin URL could be stored and used directly to construct a <link rel=stylesheet> element, even when no <meta name=sap-allowed-theme-origins> tag was present in the document. The same bypass was reachable via the ?sap-themeRoot URL parameter.Exploitation requires attacker-influenced input (e.g., a URL query parameter, tenant configuration, or user-supplied setting) to reach setThemeRoot(). A successful exploit allows an attacker to inject arbitrary CSS into the victim page, enabling:- UI redressing and clickjacking- Phishing overlays- Visual defacement- Limited data exfiltration via CSS attribute selectors targeting predictable DOM content |
| CVE-2026-55590 | CakePHP Authentication is an authentication plugin for CakePHP that can also be used in PSR-7 based applications. Prior to 2.11.1, 3.3.6, and 4.1.1, the getLoginRedirect() method contains a weakness to backslash bypasses that allows redirect targets with attacker-controlled hostnames through the redirect query string parameter. This issue is fixed in versions 2.11.1, 3.3.6, and 4.1.1. |
| CVE- | |

| | |
|---|---|
| 2026-10770 | Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Anti-Spam by CleanTalk allows Reflected XSS. This issue affects Anti-Spam by CleanTalk versions: from 0.0.0 to 9.7.1. |
| CVE-2026-55877 | Symfony UX is a JavaScript ecosystem for Symfony. From 2.17.0 before 2.36.1 and from 3.0.0 before 3.2.0, the ux_icon() Twig function is marked is_safe=['html'] and Icon::toHtml() inlines SVG source verbatim, allowing unsanitized local SVG files or Iconify on-demand JSON body responses containing nested script elements, on* event handlers, or dangerous URL schemes to execute cross-site scripting. This issue is fixed in versions 2.36.1 and 3.2.0. |
| CVE-2026-13231 | Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Advanced Content Feedback (aka admin_feedback) allows Stored XSS. This issue affects Advanced Content Feedback (aka admin_feedback) versions: from 0.0.0 to 2.8.0. |
| CVE-2026-15127 | Inappropriate implementation in WebGL in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-15128 | Inappropriate implementation in Forms in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-13234 | Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal AI (Artificial Intelligence) allows Cross-Site Scripting (XSS). This issue affects AI (Artificial Intelligence) versions: from 0.0.0 to 1.2.17, from 1.3.0 to 1.3.8, from 1.4.0 to 1.4.3. |
| CVE-2026-13334 | The Mang Board WP plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'stag' parameter in all versions up to, and including, 2.3.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. |
| CVE-2026-49971 | Laravel-Mediable before 7.0.0 contains a stored cross-site scripting vulnerability that allows authenticated or anonymous users to execute arbitrary JavaScript by uploading unsanitized SVG files containing embedded scripts in onload event handlers, script tags, or foreignObject elements. Attackers can store persistent XSS payloads in uploaded SVG files that execute with full DOM access when victims open or preview the file, enabling session cookie theft, CSRF token capture, and account takeover. |
| CVE-2026-61501 | Rejetto HFS 3.0.0 through 3.2.0 renders log entries in the administration panel as HTML without sanitization. A remote unauthenticated attacker can submit a failed login with a crafted username that is written to the error log and executes JavaScript in an administrator's browser when the logs are viewed, allowing the attacker to create accounts or execute code on the server with the administrator's privileges. |
| CVE-2026-44759 | SAP NetWeaver Enterprise Portal allows an unauthenticated attacker to inject malicious scripts into a URL parameter. The scripts are reflected in the server response and executed in a user's browser when the crafted URL is visited, leading to theft of session information, manipulation of portal content, or user redirection, resulting in a low impact on the application's confidentiality and integrity, with no impact on availability. |
| CVE-2026-0279 | Multiple cross site scripting vulnerabilities in the User-ID™ Authentication Portal (aka Captive Portal) service, GlobalProtect™ gateway/portal features and Clientless VPN of Palo Alto Networks PAN-OS® software enables a malicious unauthenticated user to store or execute malicious JavaScript payload. The security risk posed by this issue is minimized when the management interface and access to the User-ID™ Authentication Portal is restricted to only trusted internal IP addresses according to our recommended best practice deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series). Cloud NGFW is not affected by this vulnerability. |
| CVE-2026-60103 | Blender 3.0.0 through 5.1.2 contains an out-of-bounds read vulnerability that allows attackers to trigger a crash or read adjacent heap memory by supplying a crafted .blend file with a malicious signed short member_index value in the SDNA block. The member_index field is used as an array index into the sdna->members[] array in sdna_expand_names() without bounds validation, allowing any value outside the allocated range to produce an invalid pointer subsequently passed to strlen(), resulting in a SIGSEGV crash or unintended heap memory disclosure. |
| CVE-2026-58303 | Stack-based buffer overflow vulnerability in Samsung Open Source Escargot allows Overflow Buffers. This issue affects Escargot: before b30b63fc63b403907d8137da1c65aaa4521fe74e. |
| CVE-2026-58304 | Out-of-bounds read, Out-of-bounds write vulnerability in Samsung Open Source Escargot allows Overflow Buffers. This issue affects Escargot: before 779f6bedf58f334dec64b0a51ebb724b4708b84a. |
| CVE-2026-58305 | Access of resource using incompatible type ('type confusion') vulnerability in Samsung Open Source Escargot allows Pointer Manipulation. This issue affects Escargot: before 779f6bedf58f334dec64b0a51ebb724b4708b84a. |
| CVE-2026-58306 | Heap-based buffer overflow vulnerability in Samsung Open Source Escargot allows Overflow Buffers. This issue affects Escargot: before ef525f337fafddecde77a3c426212a84bb20cb98. |
| CVE-2026-58307 | Out-of-bounds read, Reachable assertion vulnerability in Samsung Open Source Escargot allows Overread Buffers, Input Data Manipulation. This issue affects Escargot: before 2dee22f5c7b8bf31cb7252d7731fae8c07f2842c. |
| CVE-2026-58587 | Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Drupal Canvas allows Cross-Site Scripting (XSS). This issue affects Drupal Canvas versions: from 0.0.0 to 1.4.2, from 1.5.0 to 1.5.2, from 1.6.0 to 1.6.1, from 1.7.0 to 1.7.1. |
| CVE-2026-59946 | Composer is a dependency Manager for the PHP language. Prior to 2.2.29 and 2.10.2, a Composer package bin entry containing .. path segments can resolve outside the package install directory and cause Composer's binary installation flow to chmod an existing host file to a world-readable and world-executable mode during composer install, update, or require. This issue is fixed in versions 2.2.29 and 2.10.2. |
| CVE-2026-11392 | The WP Hotel Booking plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'check_in_date' and 'check_out_date' parameters in all versions up to, and including, 2.3.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. |
| CVE-2026-49174 | Missing authentication for critical function in Microsoft Windows DNS allows an authorized attacker to perform tampering locally. |

| | |
|---|---|
| CVE-2026-15297 | The Newsletter, SMTP, Email marketing and Subscribe forms by Brevo (formely Sendinblue) plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the page parameter in all versions up to, and including, 3.1.77 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. |
| CVE-2026-10551 | The Breeze Cache WordPress plugin before 2.5.6 is vulnerable to unauthenticated Stored Cross-Site Scripting (XSS) due to a predictable replacement hash used during the HTML minification process and abusing a regular expression. This allows an attacker to inject arbitrary HTML attributes in the final HTML output by anticipating the placeholder format. |
| CVE-2026-15552 | Enterprise Cloud Database developed by Ragic has a Stored Cross-Site Scripting vulnerability, allowing unauthenticated remote attackers to inject persistent JavaScript code executed in users' browsers upon page load. |
| CVE-2026-60092 | AVideo (Meet plugin) through commit e8d6119f3cb1b849149906efeb0a41fc024f59f8 contains a stored cross-site scripting vulnerability in the Meet plugin's getMeetInfo.json.php endpoint. When a participant joins a public meeting, the raw HTTP User-Agent header is stored (meet_join_log.user_agent) without sanitization (bypassing AVideo's setter-level xss_esc() layer) and later echoed without output encoding (no htmlspecialchars()) in the Participants management panel, which is accessible to the meeting host and site administrators. An anonymous, unauthenticated attacker can join any public meeting while supplying a User-Agent header containing an HTML/JavaScript payload; the payload is persisted and executes in the privileged, authenticated browser session of the meeting host or a site administrator when they open the participant list. The issue was unpatched at the time of the report. |
| CVE-2026-23573 | An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability [CWE-79] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.6, FortiOS 7.4 all versions, FortiOS 7.2 all versions, FortiPAM 1.8.0, FortiPAM 1.7 all versions, FortiPAM 1.6 all versions, FortiPAM 1.5 all versions, FortiPAM 1.4 all versions, FortiPAM 1.3 all versions, FortiPAM 1.2 all versions, FortiPAM 1.1 all versions, FortiPAM 1.0 all versions, FortiProxy 7.4.0 through 7.4.3, FortiProxy 7.2.0 through 7.2.9 may allow an authenticated remote user to execute code or commands via crafted requests. |
| CVE-2026-9838 | The ICS Calendar plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'htmltagtitle' parameter in all versions up to, and including, 12.0.9 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. The vulnerability is reachable via the unauthenticated wp_ajax_nopriv_r34ics_ajax AJAX action, which accepts attacker-controlled js_args values merged over stored shortcode configuration without nonce verification, allowing the htmltagtitle key to bypass the normal shortcode allowlist check. |
| CVE-2026-50383 | Buffer over-read in Windows Print Spooler Components allows an authorized attacker to disclose information locally. |
| CVE-2026-10663 | In Zephyr's experimental USB host stack (CONFIG_USB_HOST_STACK), usbh_device_disconnect() (subsys/usb/host/usbh_device.c) freed the root usb_device slab object without clearing the cached pointer ctx->root. The bus removal handler dev_removed_handler() (subsys/usb/host/usbh_core.c) decides what to tear down solely from ctx->root, checking only that it is non-NULL. Because UHC controller drivers (e.g. uhc_max3421e, uhc_mcux_common) synthesize UHC_EVT_DEV_REMOVED directly from physical bus line state with no debounce or state guard, an attacker with physical USB access (or a rogue device that bounces its connection) can deliver a second device-removed event after a root device disconnect. The handler then re-enters usbh_device_disconnect() with the dangling pointer, locking a mutex inside the freed object (use-after-free), removing the freed node from the device list, and calling k_mem_slab_free() on the already-freed block (double-free). If the slab block has been reissued to a newly attached device in between, this corrupts a live object. Impact is denial of service (crash) and memory corruption; the attack vector is physical/local. The flaw was introduced in v4.4.0 by the connect/disconnect refactor and is fixed by clearing ctx->root in usbh_device_disconnect() before freeing. |
| CVE-2026-59890 | setuptools is a package that allows users to download, build, install, upgrade, and uninstall Python packages. Prior to 83.0.0, FileList applied MANIFEST.in exclude, global-exclude, recursive-exclude, and prune directives by matching compiled glob patterns against on-disk file names without Unicode normalization, so on macOS APFS or HFS+ an NFD file name could bypass an NFC exclusion rule and be packed into a source distribution. This issue is fixed in version 83.0.0. |
| CVE-2026-59895 | Hono is a Web application framework that provides support for any JavaScript runtime. From 4.0.0 before 4.12.27, cx() in hono/css composes class names from plain strings but marks the result as already escaped without HTML-escaping the input, allowing untrusted className values used in a JSX class attribute during server-side rendering to break out of the attribute and inject arbitrary markup. This issue is fixed in version 4.12.27. |
| CVE-2026-59923 | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, HTMLRenderer.safe_url() does not block percent-encoded javascript URIs, allowing attacker-supplied Markdown links or images to bypass URL protections and execute script in rendered HTML. This issue is fixed in version 3.3.0. |
| CVE-2026-59926 | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.2.1, render_admonition() in src/mistune/directives/admonition.py concatenates the Admonition directive :class: option into the HTML class attribute without escaping, allowing attribute injection and cross-site scripting even when HTMLRenderer escape mode is enabled. This issue is fixed in version 3.2.1. |
| CVE-2026-59929 | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, the safe_url filter in src/mistune/renderers/html.py blocks only javascript:, vbscript:, file:, and data: schemes, allowing legacy or chained schemes such as feed:, view-source:, jar:, livescript:, mocha:, ms-its:, mk:, and res: to reach rendered href and src attributes and potentially execute script in affected user agents. This issue is fixed in version 3.3.0. |
| CVE-2026-54714 | Logto is the modern, open-source auth infrastructure for SaaS and AI apps. Prior to 1.41.0, @logto/core reflected the SAML RelayState, SAMLResponse, and actionUrl into a Logto-origin auto-submit HTML form in packages/core/src/saml-application/SamlApplication/utils.ts without HTML-attribute escaping. A SAML application flow with a crafted RelayState from GET or POST /api/saml/:id/authn could inject script that runs on the Logto tenant origin after the user completes login. This issue is fixed in version 1.41.0. |
| CVE-2026-50813 | An issue in SQLite before Fossil check-in 869a51ae84df allows a local attacker to obtain sensitive information via the Session Extension changeset concat/changegroup merge path |
| CVE-2026-58588 | Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Drupal Canvas allows Cross-Site Scripting (XSS). This issue affects Drupal Canvas versions: from 0.0.0 to 1.4.2, from 1.5.0 to 1.5.2, from 1.6.0 to 1.6.1, from 1.7.0 to 1.7.1. |
| CVE-2026-55461 | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, the user edit flow stores url()->previous() from the attacker-controlled Referer header into Laravel’s intended URL session value and later uses redirect()->intended(...) when redirect_option=back is submitted, allowing Snipe-IT to be used as a trusted redirector after a legitimate user edit action. This issue is fixed in version 8.6.2. |
| CVE-2026-5793 | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Inrove Software and Internet Services BiEticaret allows Reflected XSS. This issue affects BiEticaret: before v3.3.57. |
| CVE- | Coturn is a free open source implementation of TURN and STUN Server. Prior to 4.13.0, the psd print sessions dump CLI command in coturn takes a filename argument and directly passes it to fopen with no path validation. An authenticated admin with CLI access can overwrite arbitrary files writable by the coturn |

| | |
|---|---|
| 2026-53449 | process because the command string is used as-is after stripping the psd prefix and leading spaces, allowing truncation and overwrite with session dump data. This issue is fixed in version 4.13.0. |
| CVE-2026-11567 | The SureForms WordPress plugin before 2.11.1 does not properly validate the payment amount on forms that use a dynamically-sourced (variable/hidden) payment amount, allowing unauthenticated users to underpay for the configured product or subscription. Forms using a fixed configured price are not affected. |
| CVE-2026-50324 | Loop with unreachable exit condition ('infinite loop') in Active Directory Federation Services (AD FS) allows an unauthorized attacker to deny service over a network. |
| CVE-2026-11915 | vulnerability in Drupal Brute force attack protection allows . This issue affects Brute force attack protection versions: *.*. |
| CVE-2026-15146 | GNU Wget does not validate the IP address provided by an FTP PASV response while operating in FTP passive mode. A malicious FTP server, or an HTTP server that redirects to an FTP URL, can exploit this behavior to redirect Wget’s data connection to an arbitrary IP address and port. This allows an attacker to forge server-side requests (SSRF) from the machine running Wget, potentially accessing localhost services or internal network resources. |
| CVE-2026-33794 | An Improper Check for Unusual or Exceptional Conditions vulnerability in the advanced forwarding toolkit (evo-aftmand) of Juniper Networks Junos OS Evolved on PTX Series allows an unauthenticated network-based attacker generating continuous routing updates, resulting in unilist ECMP routes, to crash the evo-aftmand process on the PFE, leading to a Denial-of-Service (DoS). The conditions required for successful exploitation are based on a sequence of events that are outside an attacker's direct control. Unified list (unilist) ECMP routes are a specific ECMP behavior where multiple equal-cost routes share a single logical next-hop list entry. The router treats them as one route with multiple next hops and load balances traffic across that unified list. Due to an issue processing unilist ECMP routing updates, internal state corruption may occur, especially in large-scale ECMP unilist deployments, leading to the evo-aftmand process crashing, resulting in an evo-aftmand-bx core. Manual intervention is required to recover by rebooting the system or restarting the FPC. This issue affects Junos OS Evolved on PTX : * from 24.4R2-EVO before 24.4R2-S3-EVO; * from 25.2 before 25.2R2-EVO. |
| CVE-2026-57022 | An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX with SPC3 and SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). When an affected device initiates a TCP connection to an attacker-controlled system that responds with a specific packet, this causes a PFE crash and restart, which affects all services until the system has automatically recovered. This issue can happen among others in the following scenarios: ALG, SSL proxy, UTM, RTLOG, AppQoE probing, AAMW, ICAP, URL filtering. This issue affects Junos OS on MX Series with SPC3, SRX5k Series with SPC3, SRX1600 Series, SRX2300 Series, SRX4000 Series, and vSRX Series: * all versions before 23.2R2-S4, * 23.4 versions before 23.4R2-S5, * 24.2 versions before 24.2R2. |
| CVE-2026-31981 | A Stored HTML Injection vulnerability was discovered in the Diagram tab and Graph view due to a shared input validation function being insufficiently restrictive. An authenticated user with administrative privileges can inject malicious HTML tags into N2OS configuration data through multiple input vectors. When a victim views the affected data in the Diagram tab and Graph view, the injected HTML renders in their browser, enabling phishing and possibly open redirect attacks. Full XSS exploitation and direct information disclosure are prevented by the existing input validation and Content Security Policy configuration. |
| CVE-2026-15087 | vulnerability in Drupal Clean RESTful allows . This issue affects Clean RESTful versions: *.*. |
| CVE-2026-15086 | vulnerability in Drupal Raw Formatter [Meta Tag Formatter] allows . This issue affects Raw Formatter [Meta Tag Formatter] versions: *.*. |
| CVE-2026-54590 | AsyncSSH is a Python package which provides an asynchronous client and server implementation of the SSHv2 protocol on top of the Python asyncio framework. Version 2.23.0 contains an incomplete fix for CVE-2026-45309 in SSHServerConfig._set_tokens that blocks /, , and .. before %u substitution in AuthorizedKeysFile but does not block a leading ~ or ${ENV}, allowing later expansion in _expand_val and Path(filename).expanduser() to escape the intended authorized-keys directory. This issue is fixed in version 2.23.1. |
| CVE-2026-11914 | vulnerability in Drupal Composer allows . This issue affects Composer versions: *.*. |
| CVE-2026-15289 | The Booking calendar, Appointment Booking System plugin for WordPress is vulnerable to time-based SQL Injection via the ‘wpdevart_id’ parameter in all versions up to, and including, 3.2.17 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. In order to exploit the vulnerability, the Pro version of the plugin must be installed and activated, with the 'Delete previous dates' option checked. |
| CVE-2026-54773 | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, CoreWCF WS-Security signature verification performs a document-wide ds:Signature lookup, allowing an unauthenticated remote attacker to place a SOAP header before wsse:Security and cause WSSecurityOneDotZeroReceiveSecurityHeader to verify an attacker-supplied signature instead of the security header signature. This issue is fixed in versions 1.8.1 and 1.9.1. |
| CVE-2026-57030 | A Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in the packet forwarding engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). As part of the stateful traffic processing on SRX Series devices flows are being established, and removed when not needed anymore. During the removal process the timeout of a flow should be set to 3 seconds and consequentially the flow should be removed shortly after. Due to a race condition occurring when setting the timeout there is a chance (the exact conditions are outside the attackers control) that the timeout is instead set to a very high value of larger than 10,000 seconds: user@host> show security flow session \| match timeout Session ID: 98784248524, Policy name: PROD-FLOW/4, HA State: Active, Timeout: 85250, Session State: Valid This will lead to an accumulation of flows which can be observed by an ever-increasing value of invalidated sessions in the output of 'show security flow session summary': user@host> show security flow session summary \| match invalid Invalidated sessions: 216931These sessions can't be cleared manually with the 'clear security flow session' command, which will either lead to forwarding to stop (and the system needs to be manually recovered with a reboot) or to a flowd core and automatic reboot. This issue affects Junos OS on SRX Series: * 24.2 versions before 24.2R2-S3, * 24.4 versions before 24.4R2-S1, 24.4R2-S2, * 25.2 versions before 25.2R1-S2, 25.2R2. This issue does not affect releases earlier than 24.2R1; |
| CVE-2026-54779 | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, CoreWCF SAML token replay protection is inoperative because DefaultTokenReplayCache.TryAdd does not reject duplicate tokens when DetectReplayedTokens is enabled, allowing a captured token to be reused. This issue is fixed in versions 1.8.1 and 1.9.1. |
| CVE-2026-59999 | In sshd in OpenSSH before 10.4, DisableForwarding=yes was supposed to take precedence over PermitTunnel=yes, but did not. |

| | |
|---|---|
| CVE-2026-9571 | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to invalidate OAuth refresh tokens upon user account deactivation, which allows a deactivated user or an attacker in possession of a valid refresh token to obtain new functional access tokens via the OAuth refresh token grant endpoint.. Mattermost Advisory ID: MMSA-2026-00680 |
| CVE-2026-58501 | Zeep is a Python SOAP client. From 4.0.0 before 4.3.3, Settings.forbid_external is defined but not enforced when parsing WSDL or XSD documents, allowing transitive xsd:import, xsd:include, wsdl:import, and lxml entity or DTD references to fetch attacker-chosen HTTP or HTTPS URLs. This issue is fixed in version 4.3.3. |
| CVE-2026-59924 | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, Include.parse() joins and normalizes user-supplied include paths without verifying that the result remains within the intended markdown directory, allowing crafted include paths to access files outside that directory when markdown files are processed using md.read(). This issue is fixed in version 3.3.0. |
| CVE-2026-49844 | Improper encoding of non-finite floating-point values during MapMessage JSON serialization in Apache Log4j API produces output that is not valid JSON. This issue affects Apache Log4j API versions 2.13.1 through 2.25.4 and version 2.26.0. The fix for CVE-2026-34481 did not cover all code paths: when a MapMessage contains a non-finite IEEE 754 value (NaN, Infinity, or -Infinity), MapMessage.asJson() emits the corresponding bare token. RFC 8259 does not permit these tokens, so a conformant parser rejects the resulting document. The defect is reachable only when both of the following conditions hold: * The application uses the message resolver https://logging.apache.org/log4j/2.x/manual/json-template-layout.html#event-template-resolver-message of JsonTemplateLayout or any other layout that relies on MapMessage.asJson() or MapMessage.getFormattedMessage(new String[]{"JSON"}). * The application logs a MapMessage that contains an attacker-controlled floating-point value. An attacker who can supply a non-finite value can cause the affected layout to emit malformed JSON, which may corrupt the enclosing log record or disrupt downstream log ingestion and parsing. Users are advised to upgrade to Apache Log4j API 2.25.5 or 2.26.1, both of which emit RFC 8259-compliant JSON for non-finite values. |
| CVE-2026-55803 | Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Drupal core allows Object Injection. This issue affects Drupal core versions: from 0.0.0 to 10.5.12, from 10.6.0 to 10.6.11, from 11.2.0 to 11.2.14, from 11.3.0 to 11.3.12, from 0.0.0 to 11.0.*, from 0.0.0 to 11.1.*. |
| CVE-2026-55804 | Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Drupal core allows Object Injection. This issue affects Drupal core versions: from 0.0.0 to 10.5.12, from 10.6.0 to 10.6.11, from 11.2.0 to 11.2.14, from 11.3.0 to 11.3.12, from 0.0.0 to 11.0.*, from 0.0.0 to 11.1.*. |
| CVE-2026-55806 | URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Drupal Drupal core allows Content Spoofing. This issue affects Drupal core versions: from 0.0.0 to 10.5.12, from 10.6.0 to 10.6.11, from 11.2.0 to 11.2.14, from 11.3.0 to 11.3.12, from 0.0.0 to 11.0.*, from 0.0.0 to 11.1.*. |
| CVE-2026-55761 | Portainer Community Edition is a lightweight service delivery platform for containerized applications that can be used to manage Docker, Swarm, Kubernetes and ACI environments. In versions 2.39.0 through 2.39.3 and 2.40.0 until 2.43.0, unauthenticated restore and administrator initialization endpoints (/api/restore and /api/users/admin/init) remain accessible during the five-minute setup window for uninitialized instances, allowing a network attacker to restore a crafted backup or create the first administrator account and gain full administrative access. This issue is fixed in versions 2.39.4 and 2.43.0. |
| CVE-2026-57691 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Eli Anti-Malware Security and Brute-Force Firewall gotmls allows Reflected XSS.This issue affects Anti-Malware Security and Brute-Force Firewall: from n/a through <= 4.23.89. |
| CVE-2026-55438 | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.17, 2.32.7, 2.33.8, and 2.34.2, Coder's subdomain-based workspace app proxy allowed the same-owner CORS check to be bypassed. When a workspace-name subdomain segment parsed as a UUID, the workspace was resolved by ID without confirming the URL's username matched the real owner, while the CORS middleware trusted the unverified username in the hostname. Practical exploitation requires subdomain app routing (wildcard hostname) enabled and a victim who visits the attacker's crafted app URL while authenticated. The fix in versions 2.29.17, 2.32.7, 2.33.8, and 2.34.2 validates the subdomain username against the resolved workspace's actual owner and bases the same-owner CORS decision on the authoritative owner identity. No known workarounds are available. |
| CVE-2026-52761 | ModSecurity is an open source, cross platform web application firewall (WAF) engine for Apache, IIS and Nginx. From 3.0.0 through 3.0.15, the t:utf8toUnicode transformation in src/actions/transformations/utf8_to_unicode.cc produces wrong output on i386 architecture because snprintf uses sizeof on a char pointer rather than the length of the unicode buffer, allowing rules that use this transformation to be bypassed on i386 architecture. This issue is fixed in version 3.0.16. |
| CVE-2026-55187 | Mailpit is an email testing tool and API for developers. Prior to 1.30.2, the remediation shipped for CVE-2026-27808 is incomplete because the tools.IsInternalIP deny-list in internal/tools/net.go relies on Go's standard library classification helpers and does not block IPv6 transition mechanisms or prefixes such as NAT64, 6to4, IPv4-compatible IPv6, ISATAP, fec0::/10, and 2001:db8::/32. An attacker who can deliver email and invoke POST /api/v1/message/{ID}/link-check can coerce the Link Check API's safeDialContext path into dialing internal destinations and can use status-code and error feedback to map internal service reachability, including cloud metadata endpoints. This issue is fixed in version 1.30.2. |
| CVE-2026-55430 | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, the workspace app proxy resolves the target app from `httpapi.RequestHost()` which prefers the `X-Forwarded-Host` header over the real `Host` header. No middleware strips `X-Forwarded-Host` before routing and the header is not browser-forbidden so client-side JavaScript can set it on `fetch()` calls. Practical exploitation requires subdomain app routing (wildcard hostname) enabled, a victim who visits the attacker's shared app and a deployment whose upstream proxy does not strip `X-Forwarded-Host`. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 trusts `X-Forwarded-Host` only from configured trusted proxies and otherwise resolves the routing host from the verified request host. As a workaround, place an upstream reverse proxy that strips or overwrites `X-Forwarded-Host` on untrusted requests. |
| CVE-2026-57054 | A Use of Incorrectly-Resolved Name or Reference vulnerability in the URL filtering plugin of Juniper Networks Junos OS on MX Series allows an unauthenticated, network-based attacker to bypass web filtering and access downstream resources that should be unreachable. If an MX Series device is configured with web filtering, and an attacker sends a request with a specifically formatted URL, this request will get forwarded despite the system being configured to block it. In turn, an attacker can access downstream resources that are expected to be unreachable. This issue affects Junos OS on MX Series: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S5, * 24.4 versions before 24.4R2-S4, * 25.2 versions before 25.2R2-S1, * 25.4 versions before 25.4R1-S2, 25.4R2. |
| CVE-2026-55475 | Snipe-IT is an IT asset/license management system. Prior to 8.6.1, the Importer API endpoint allows a user with CSV import capabilities and a valid API key to overwrite the created_by value of an import file, allowing unauthorized modification of import ownership metadata. This issue is fixed in version 8.6.1. |
| CVE-2026-31267 | Mercusys MW302R MW302R(EU)_V1_1.4.10 Build 231023 is vulnerable to Buffer Overflow in the administrative web interface. A stack buffer overflow vulnerability in the administrative web interface allows an authenticated attacker with administrative privileges to trigger a system crash by sending a specially crafted request. The vulnerability results in denial of service through control flow manipulation to an arbitrary instruction address. |
| CVE-2026-61432 | PraisonAI (praisonaiagents) before 1.6.78 contains a path traversal vulnerability in the FastContext feature (praisonaiagents.context.fast). FastContextAgent.execute_tool() prepends the configured workspace_path only for relative paths and neither rejects absolute paths nor canonicalizes joined paths before enforcing workspace containment. As a result, tool arguments or model-generated function calls to grep_search, glob_search, read_file, or list_directory can supply absolute paths or '../' traversal sequences to read, search, and enumerate files outside the intended workspace directory, with file contents returned to the |

| | |
|---|---|
| | caller or injected into the model's tool-result context. |
| CVE-2026-15516 | A vulnerability was detected in MacCMS Pro up to 2022.1000.3005. Impacted is the function step5 of the file application/install/controller/Index.php of the component Installation Module. The manipulation results in authorization bypass. The attack may be launched remotely. The attack requires a high level of complexity. The exploitability is considered difficult. The exploit is now public and may be used. Upgrading to version 2022.1000.3025 is recommended to address this issue. Upgrading the affected component is recommended. |
| CVE-2026-47969 | Audition is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file. |
| CVE-2026-48580 | Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to disclose information locally. |
| CVE-2026-59839 | A improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiOS 7.6.0 through 7.6.6, FortiOS 7.4.0 through 7.4.9, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions, FortiPAM 1.8.0, FortiPAM 1.7.0 through 1.7.2, FortiPAM 1.6 all versions, FortiPAM 1.5 all versions, FortiPAM 1.4 all versions, FortiPAM 1.3 all versions, FortiPAM 1.2 all versions, FortiPAM 1.1 all versions, FortiPAM 1.0 all versions, FortiProxy 7.6.0 through 7.6.5, FortiProxy 7.4 through 7.4.13, FortiProxy 7.2 all versions, FortiProxy 7.0 all versions may allow attacker to execute unauthorized code or commands via <insert attack vector here> |
| CVE-2026-44769 | SAP S/4HANA application Project Management (PPM-PRO) allows an attacker with high privileges to execute crafted database queries, exposing the backend database. This results in low impact on confidentiality, with no impact on integrity and availability of the application. |
| CVE-2026-58614 | Out-of-bounds read in Windows Kernel allows an authorized attacker to bypass a security feature locally. |
| CVE-2026-50408 | Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally. |
| CVE-2026-56288 | GNU patch is vulnerable to a NULL pointer dereference when processing a specially crafted unified-diff patch file. Improper handling of consecutive end-of-file newline markers can corrupt internal hunk (single block of changes in diff) data structures, causing the application to pass a NULL pointer to fwrite() during patch processing. An attacker can trigger this condition with a malicious patch file, causing the utility to crash and resulting in a denial of service. This issue has been fixed in the commit e6d6a4e021660679d7fc9150f981d4920f722313 |
| CVE-2026-50409 | Exposure of sensitive information to an unauthorized actor in Windows Overlay Filter allows an authorized attacker to disclose information locally. |
| CVE-2026-56289 | GNU patch is vulnerable to a denial of service (DoS) due to improper validation of hunk (single block of changes in diff) line offsets in unified-diff input. A specially crafted patch can specify an extremely large line number, causing the application to enter an effectively infinite processing loop while attempting to locate the requested position. This results in excessive CPU consumption and prevents the process from completing. An attacker can trigger this behavior by supplying a malicious patch file, causing the utility to become unresponsive and require manual termination. This issue has been fixed in the commit faba04ef4f2b410257f76c1b9dc85e350929c4b9 |
| CVE-2026-49177 | Out-of-bounds read in Windows TCP/IP allows an authorized attacker to disclose information locally. |
| CVE-2026-15169 | UMTS FP protocol dissector crash in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service |
| CVE-2026-50401 | Out-of-bounds read in Windows Cloud Files Mini Filter Driver allows an authorized attacker to disclose information locally. |
| CVE-2026-15682 | AnyDesk Support Information Link Following Denial-of-Service Vulnerability. This vulnerability allows local attackers to create a denial-of-service condition on affected installations of AnyDesk. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Send Support Information feature. By creating a junction, an attacker can abuse the service to create arbitrary files. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-26645. |
| CVE-2026-44512 | Open Neural Network Exchange (ONNX) is an open standard for machine learning interoperability. From 1.9.0 before 1.22.0, onnx.version_converter.convert_version() can dereference a null pointer in Upsample_6_7::adapt_upsample_6_7() in onnx/version_converter/adapters/upsample_6_7.h when processing an untrusted model with an Upsample node that has zero inputs, causing an unrecoverable denial of service. This issue is fixed in version 1.22.0. |
| CVE-2026-50352 | Exposure of sensitive information to an unauthorized actor in Windows Cryptographic Services allows an authorized attacker to disclose information locally. |
| CVE-2026-50377 | Out-of-bounds read in Windows Kernel allows an authorized attacker to elevate privileges locally. |
| CVE-2026-50341 | Buffer over-read in Windows NTFS allows an authorized attacker to disclose information locally. |
| CVE-2026-50339 | Exposure of sensitive information to an unauthorized actor in Windows Push Notifications allows an authorized attacker to disclose information locally. |
| CVE-2026- | Exposure of sensitive information to an unauthorized actor in Windows Notification allows an authorized attacker to disclose information locally. |

| | |
|---|---|
| 50334 | |
| CVE-2026-15163 | Multiple protocol dissector infinite loops in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allow denial of service |
| CVE-2026-15164 | Crash in ciscodump 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service |
| CVE-2026-15165 | TLS ECH decryptor crash in Wireshark 4.6.0 to 4.6.6 allows denial of service |
| CVE-2026-15166 | IEEE 802.11 protocol dissector crash in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service |
| CVE-2026-50389 | Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally. |
| CVE-2026-50394 | Exposure of sensitive information to an unauthorized actor in Windows Media allows an authorized attacker to disclose information locally. |
| CVE-2026-15170 | Z39.50 protocol dissector crash in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service |
| CVE-2026-15171 | SSH protocol dissector crash in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service |
| CVE-2026-15172 | FMP/NOTIFY protocol dissector crash in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service |
| CVE-2026-15174 | Catapult DCT2000 protocol dissector crash in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows denial of service |
| CVE-2026-15681 | AnyDesk Screen Recording Link Following Denial-of-Service Vulnerability. This vulnerability allows local attackers to create a denial-of-service condition on affected installations of AnyDesk. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of screen recording files. By creating a junction, an attacker can abuse the service to create arbitrary files. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-26591. |
| CVE-2026-60088 | PraisonAI before 4.6.78 fails to validate file path references in custom command templates, allowing attackers to read files outside the workspace. Attackers can include path traversal sequences like @../outside_secret.txt or absolute paths in project command files to exfiltrate process-readable files into model prompts. |
| CVE-2026-50812 | A NULL pointer dereference in the SQLite Session Extension in SQLite 3.53.1 and SQLite trunk builds before check-in e807d4e3798efd53 allows an attacker who can supply a malformed changeset blob to cause a denial of service. The issue occurs when sqlite3changeset_apply_v3() applies a corrupt changeset and reaches sqlite3_value_type() with a NULL sqlite3_value pointer. |
| CVE-2026-49801 | Use of uninitialized resource in Windows SMB allows an authorized attacker to disclose information locally. |
| CVE-2026-54997 | Use of uninitialized resource in Windows SMB allows an authorized attacker to disclose information locally. |
| CVE-2026-33802 | A Missing Authorization vulnerability in the CLI of Juniper Networks Junos OS on EX Series allows a local, authenticated attacker to cause a Denial-of-Service (DoS). On EX2300, EX4000, EX4100, EX4300-MP (Multigigabit) and EX4400 switches, an authenticated, local attacker with no specific permissions or class can execute a specific, privileged CLI 'request' command which will cause complete traffic impact until the system automatically recovers. This issue affects Junos OS on EX2300, EX4000, EX4100, EX4300-MP (Multigigabit) and EX4400: * 23.2R2 versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S3, * 25.2 versions before 25.2R2, * 25.4 versions before 25.4R1-S1. |
| CVE-2026-50295 | Improper privilege management in Microsoft Windows DNS allows an authorized attacker to bypass a security feature locally. |
| CVE-2026-41087 | Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally. |
| CVE-2026-15551 | Integer overflow or wraparound vulnerability in Samsung Open Source rlottie allows Overflow Buffers. This issue affects . |
| CVE-2026-10670 | The CONFIG_USERSPACE verification handler for the k_thread_name_copy() system call (z_vrfy_k_thread_name_copy() in kernel/thread.c) calls k_object_find() on the caller-supplied thread pointer and then dereferences the returned struct k_object without checking it for NULL. k_object_find() returns NULL whenever the supplied pointer is not a registered (static or dynamic) kernel object. The pre-fix guard tested thread == NULL instead of ko == NULL, so an unprivileged user-mode thread that invokes k_thread_name_copy() with any non-NULL but unregistered pointer (e.g. an arbitrary address) passes the NULL test, after which the verifier reads ko->type through a NULL pointer. Because the syscall verifier runs in supervisor mode, this NULL dereference is a kernel-mode fault that halts or reboots the system, allowing untrusted user code to crash the kernel across the userspace security boundary (denial of service). The marshaller passes the thread |

| | |
|---|---|
| | argument to the verifier without any prior K_SYSCALL_OBJ validation, so the bad pointer reaches the defect directly. The flaw affects builds with CONFIG_USERSPACE and CONFIG_THREAD_NAME enabled and has been present since the special-case lookup was introduced around v2.0.0; it is present in v4.4.0 and earlier. The fix changes the guard to check the k_object_find() return value (ko == NULL) before dereferencing it. |
| CVE-2026-57025 | A Return of Pointer Value Outside of Expected Range vulnerability in the fileio library of Juniper Networks Junos OS and Junos OS Evolved allows a local, low-privilged attacker to cause a Denial-of-Service (DoS). On EX Series, QFX Series and MX Series a low-privileged attacker issuing a specific 'show l2-learning' command will cause an l2ald crash which will lead to a temporary service impact for all layer 2 services until the process has automatically restarted. This issue affects EX Series, QFX Series, MX Series: Junos OS: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S7, * 24.2 versions before 24.2R2, * 24.4 versions before 24.4R1-S2. Junos OS Evolved: * all versions before 23.2R2-S7-EVO, * 23.4 versions before 23.4R2-S8-EVO, * 24.2 versions before 24.2R2-EVO, * 24.4 versions before 24.4R1-S3-EVO. |
| CVE-2026-50430 | Exposure of sensitive information to an unauthorized actor in Windows Push Notifications allows an authorized attacker to disclose information locally. |
| CVE-2026-34349 | Exposure of sensitive information to an unauthorized actor in Windows Media allows an authorized attacker to disclose information locally. |
| CVE-2026-50431 | Windows Quality of Service (QoS) Packet Scheduler Information Disclosure Vulnerability |
| CVE-2026-45496 | Improper limitation of a pathname to a restricted directory ('path traversal') in Visual Studio Code allows an unauthorized attacker to bypass a security feature locally. |
| CVE-2026-59857 | Vim is an open source, command line text editor. Prior to 9.2.0725, the single-byte branch of spell_soundfold_sal() in src/spell.c translates a word through a spell file's SAL sound-folding rules into a caller-owned result buffer, but its result writes are guarded with reslen < MAXWLEN, allowing reslen to reach MAXWLEN before res[reslen] = NUL writes one byte past the end of the MAXWLEN-element stack buffer. A boundary-length word passed to soundfold(), or reached via sound-based spell suggestion while a SAL-based spell language is active under a non-multibyte 8-bit encoding, can corrupt the eval_soundfold() stack frame and crash the editor. This issue is fixed in version 9.2.0725. |
| CVE-2026-50434 | Exposure of sensitive information to an unauthorized actor in Windows Push Notifications allows an authorized attacker to disclose information locally. |
| CVE-2026-49180 | Improper link resolution before file access ('link following') in Universal Plug and Play (upnp.dll) allows an authorized attacker to disclose information locally. |
| CVE-2026-50437 | Out-of-bounds read in Windows DWM Core Library allows an authorized attacker to disclose information locally. |
| CVE-2026-40422 | Use of uninitialized resource in Windows File Explorer allows an authorized attacker to disclose information locally. |
| CVE-2026-39243 | decompress before 4.2.2 allows arbitrary hardlink creation during archive extraction, enabling file read disclosure and file corruption. When processing hardlink entries (type === 'link'), the x.linkname field from the archive is passed directly to fs.link() without validation (index.js line 113). An attacker can craft an archive with a hardlink entry whose linkname is an absolute path to any file on the same filesystem. This creates a hardlink inside the extraction directory that shares the same inode as the target file, enabling both reading and overwriting the original file's content. Hardlinks are limited to files on the same filesystem and cannot target directories. |
| CVE-2026-50300 | Integer underflow (wrap or wraparound) in Windows Kernel allows an authorized attacker to disclose information locally. |
| CVE-2026-50316 | Insertion of sensitive information into log file in Windows Kernel allows an authorized attacker to disclose information locally. |
| CVE-2026-50456 | Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally. |
| CVE-2026-50455 | Use of uninitialized resource in Universal Plug and Play (upnp.dll) allows an authorized attacker to disclose information locally. |
| CVE-2026-61431 | PraisonAI before 4.6.78 contains a path traversal vulnerability in ContextGatherer that fails to validate include paths in .praisoncontext and .praisoninclude files. Attackers can supply absolute paths or parent directory traversal sequences to read arbitrary files outside the workspace and include their contents in the generated context bundle. |
| CVE-2026-50381 | Access of resource using incompatible type ('type confusion') in Composite Image File System Driver allows an authorized attacker to disclose information locally. |
| CVE-2026-58198 | ChatterBot is a machine learning, conversational dialog engine for creating chat bots. Prior to 1.2.14, UbuntuCorpusTrainer.extract() uses a predictable home-rooted output directory (~/ubuntu_data/ubuntu_dialogs) with a check-then-create pattern followed by tar.extractall(path=self.data_path), allowing a local attacker who pre-plants a symlink at the predictable path to cause archive contents to be written through the symlink to an attacker-chosen directory. This issue is fixed in version 1.2.14. |
| CVE-2026-50350 | Exposure of sensitive information to an unauthorized actor in Windows Trusted Runtime Interface Driver allows an authorized attacker to disclose information locally. |

| | |
|---|---|
| CVE-2026-60089 | PraisonAI (pip package praisonaiagents) before 1.6.78 automatically loads defaults from a project-local .praisonai/config.toml when constructing an Agent, and does not validate the defaults.output.output_file path. A repository-controlled config file can set output_file to an absolute or '..' traversal path; when the developer subsequently calls agent.start() without explicitly passing an output parameter, PraisonAI writes the agent response to that path (creating parent directories as needed), allowing an untrusted checked-out project to overwrite files outside the project root with the privileges of the user running PraisonAI. |
| CVE-2026-50303 | Use of a cryptographic primitive with a risky implementation in Windows Key Guard allows an authorized attacker to bypass a security feature locally. |
| CVE-2026-33842 | Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally. |
| CVE-2026-34328 | Exposure of sensitive information to an unauthorized actor in Windows Audio Service allows an authorized attacker to disclose information locally. |
| CVE-2026-34346 | Cleartext transmission of sensitive information in Windows Ancillary Function Driver for WinSock allows an authorized attacker to disclose information locally. |
| CVE-2026-50442 | Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally. |
| CVE-2026-44918 | OpenStack Ironic through before 37.0.1 allows creation or modification of nodes cross-project without authorization. |
| CVE-2026-15082 | Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Siteimprove Analytics allows Cross-Site Scripting (XSS). This issue affects Siteimprove Analytics versions: from 0.0.0 to 2.0.1. |
| CVE-2026-15084 | Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal UI Patterns (SDC in Drupal UI) allows Stored XSS. This issue affects UI Patterns (SDC in Drupal UI) versions: from 2.0.0 to 2.0.17. |
| CVE-2026-60119 | Hi.Events before 1.11.0 contains a cross-site scripting vulnerability that allows authenticated attackers with event creation or edit permissions to inject arbitrary HTML and JavaScript by embedding a malicious event title containing the </script> sequence, which is not escaped by JSON.stringify() when embedded in inline script tags. Attackers can craft an event title that breaks out of the script context in the application/ld+json structured data block or server-side rehydrated state, causing the payload to execute in the browser of any user who views the public event page, including unauthenticated visitors and authenticated administrators. |
| CVE-2026-15079 | Improper Restriction of Excessive Authentication Attempts vulnerability in Drupal Login Disable allows Brute Force. This issue affects Login Disable versions: from 0.0.0 to 2.1.4. |
| CVE-2026-15085 | Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal AI SEO/GEO Analyzer allows Stored XSS. This issue affects AI SEO/GEO Analyzer versions: from 0.0.0 to 1.1.3. |
| CVE-2026-61504 | Rejetto HFS 3.0.0 through 3.2.0 does not escape file names in its fallback "basic" web listing, and this listing can be forced by any browser via the ?get=basic parameter. A user with upload permission - or an anonymous user on servers with an open upload folder - can store a file whose name contains script that executes in the browser of anyone viewing the listing. |
| CVE-2026-15331 | A vulnerability was identified in zhayujie CowAgent up to 2.1.0. The affected element is the function _add_url/_add_package of the file agent/skills/service.py of the component Skill Installation Handler. The manipulation of the argument Name leads to path traversal. The attack may be initiated remotely. Upgrading to version 2.1.2 is sufficient to fix this issue. The identifier of the patch is e85290cddcbb5ffc9c235927f4c92e5b4c3ec264. It is advisable to upgrade the affected component. |
| CVE-2026-5069 | The Fluent Forms plugin for WordPress is vulnerable to incorrect authorization via the 'subscription_id' parameter in versions up to, and including, 6.2.1. This is due to insufficient ownership authorization checks in the payment cancellation AJAX flow. This makes it possible for authenticated attackers, with subscriber-level access and above, to submit cancellation requests for other users' subscriptions. |
| CVE-2025-15665 | The Ultimate Before After Image Slider & Gallery WordPress plugin before 4.7.1 does not escape the value of the BEAF Slider widget's shortcode field before outputting it on the front end (the value is passed through do_shortcode, which echoes non-shortcode content verbatim), allowing users with administrator-level access to store a script that executes in the browser of any visitor who loads a page displaying the widget. |
| CVE-2026-11818 | The WPCafe – Restaurant Menu, Online Food Ordering & Table Booking System plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.0.14. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to list, create, update, delete, clone, and bulk-delete notification flow workflows that are intended to be managed only by administrators. The only protection on these endpoints is a wp_rest nonce check, which is obtainable by any logged-in user from the frontend page source. |
| CVE-2026-57214 | RabbitMQ is a messaging and streaming broker. Prior to 4.2.5, the RabbitMQ management UI renders the x-internal-purpose queue or exchange argument into an HTML title attribute without proper escaping on the Queues and Exchanges pages, allowing a user with permission to declare a queue or exchange to execute JavaScript in another user's browser. This issue is fixed in version 4.2.5. |
| CVE-2026-59212 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.6 before 0.10.0, _verify_knowledge_file_access only checked read access while file write and delete routes later trusted object-derived access through writable model meta.knowledge entries, allowing a user with read-only knowledge file access to upgrade to file write or delete operations. This issue is fixed in version 0.10.0. |
| CVE-2026-59225 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.8.12 before 0.10.0, an authenticated non-admin user with read access to an arena wrapper model can reach a restricted underlying model through task endpoints such as /api/v1/tasks/moa/completions. The normal chat route resolves arena models before the final chat dispatch and therefore re-checks the selected underlying model. The task routes call utils.chat.generate_chat_completion() directly. In that direct path, arena fallback resolution happens after the wrapper access check and then recurses with bypass_filter=True, skipping the selected submodel's access check. This issue is fixed in version 0.10.0. |
| CVE-2026-56458 | HCL DevOps Deploy uses Cross-Origin Resource Sharing (CORS) which could allow an attacker to carry out privileged actions and retrieve sensitive information as the domain name is not being limited to only trusted domains. |

| | |
|---|---|
| CVE-2026-15719 | We are aware that exploit code for this is public however we are not aware of any attacks in the wild abusing this flaw. This vulnerability was fixed in Firefox 152.0.6. |
| CVE-2026-55464 | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, CommonMark escapes raw HTML but does not sanitize javascript: URIs in Markdown hyperlinks, allowing a user with assets.edit permission to place a malicious link in a markdown-textarea custom field that executes arbitrary JavaScript when another user opens the asset detail page and clicks the link. This issue is fixed in version 8.6.2. |
| CVE-2026-60120 | Bagisto before 2.4.4 contains a stored cross-site scripting vulnerability via client-side template injection that allows unauthenticated attackers to execute arbitrary JavaScript in administrator browsers by registering a customer account with malicious payload in the first or last name field. The create.blade.php template renders customer name fields without the Vue.js v-pre directive, causing Vue.js to evaluate stored template expressions as live JavaScript when an administrator opens the Create Order page for the affected customer. |
| CVE-2026-55478 | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, POST /api/v1/kits/{kit_id}/licenses checks whether the caller can edit kits but does not authorize access to the referenced license object, allowing a low-privilege user with predefined-kit permissions to bind a license they should not be able to access or manage into a kit. This issue is fixed in version 8.6.2. |
| CVE-2026-57230 | OpenReplay is a self-hosted session replay suite. Prior to 1.27.0, the session search and analytics API in enterprise editions with multi-tenancy enabled built ClickHouse queries by inserting user input into the query string, including two positions that took input without escaping, allowing an authenticated member to read any ClickHouse table through blind boolean and time-based exfiltration and to break the project's session search for all viewers until the stored key is removed. This issue is fixed in version 1.27.0. |
| CVE-2026-15320 | A vulnerability was detected in Sipeed PicoClaw up to 0.2.9. This vulnerability affects the function rt.ReloadConfig of the file pkg/channels/pico/pico.go. Performing a manipulation of the argument message.send results in missing authorization. It is possible to initiate the attack remotely. The exploit is now public and may be used. The reported GitHub issue was closed automatically due to inactivity. |
| CVE-2026-58211 | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.3 and 2.12.12, a client could be registered as the configured no_auth_user through a parser path used when the first client operation was not CONNECT, bypassing user-level connection restrictions such as allowed_connection_types or proxy_required that normal authentication would apply. This issue is fixed in versions 2.14.3 and 2.12.12. |
| CVE-2026-10769 | Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Commerce Core allows Stored XSS. This issue affects Commerce Core versions: from 3.3.0 to 3.3.6. |
| CVE-2026-53962 | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, insufficient SVG sanitization in upload and user avatar handling could lead to cross-site scripting when a user visited specific URLs that are not normally part of community browsing. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5. |
| CVE-2026-55170 | OpenFGA is an authorization/permission engine built for developers. Prior to 1.18.0, when MySQL is being used as the datastore and authorization decisions rely on case-sensitive user strings, the tuple, changelog, and authorization_model identifier columns can compare case-distinct values such as user:Alice and user:alice as equivalent, causing two distinct check requests to return the same response. This issue is fixed in 1.18.0. |
| CVE-2026-55424 | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, a topic "featured link" was not sufficiently normalized and escaped before being rendered in the topic list, allowing a user who can set a featured link to inject JavaScript when default Content Security Policy protections were modified or disabled. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5. |
| CVE-2026-56309 | Capgo before 12.128.2 fails to enforce plan/quota restrictions on the /files/upload/attachments endpoint, allowing plan-blocked apps to create publicly readable R2 objects. Attackers can upload arbitrary attachments using upload-scoped API keys that bypass plan checks, persist outside normal bundle metadata, and survive app deletion, enabling storage and bandwidth abuse. |
| CVE-2026-58144 | Cotonti Siena 0.9.26 and earlier contains a stored cross-site scripting vulnerability that allows authenticated users with PFS access to inject arbitrary script payloads by supplying malicious HTML in the ntitle parameter processed through the TXT filter in pfs.main.php. Attackers can create a folder with a crafted title containing script tags that are stored unescaped in the database and execute in the browser of any user who views the folder listing, including administrators. |
| CVE-2026-5005 | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Twiser Informatics Technology Consulting, Trade and Education Inc. OKRs & Goals allows Stored XSS. This issue affects OKRs & Goals: from 28220 before 28398. |
| CVE-2026-11908 | Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Tagify allows Stored XSS. This issue affects Tagify versions: from 0.0.0 to 1.2.52. |
| CVE-2026-8315 | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Webbeyaz Web Design Mediküm Web allows Stored XSS. This issue affects Mediküm Web: through 08072026. NOTE: The vendor was contacted and it was learned that the product is not supported. |
| CVE-2026-61968 | Missing Authorization vulnerability in Saad Iqbal myCred mycred allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects myCred: from n/a through <= 3.1.2. |
| CVE-2026-58589 | Missing Authorization vulnerability in Drupal FlowDrop allows Forceful Browsing. This issue affects FlowDrop versions: from 0.0.0 to 1.6.0. |
| CVE-2026-58590 | Missing Authorization vulnerability in Drupal FlowDrop allows Forceful Browsing. This issue affects FlowDrop versions: from 0.0.0 to 1.6.0. |
| CVE-2026-58591 | Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Colorbox allows Cross-Site Scripting (XSS). This issue affects Colorbox versions: from 0.0.0 to 2.1.5, from 0.0.0 to 2.2.0. |
| CVE-2026-56283 | Capgo before 12.128.2 contains an html injection vulnerability in the organization settings endpoint that allows attackers to inject malicious HTML content. Attackers can craft payloads in the organization name field to redirect users to untrusted websites, enabling phishing attacks and reputational damage. |
| CVE-2026- | The Tutor LMS WordPress plugin before 3.9.13 does not verify ownership of the targeted quiz attempt before writing to it, allowing authenticated users with |

| | |
|---|---|
| 12271 | subscriber-level access and above to modify and force-complete other students' quiz attempts, overwriting their recorded marks and pass/fail result. |
| CVE-2026-56252 | Capgo before 12.128.2 contains a scope isolation vulnerability in the POST /webhooks/test endpoint that allows app-scoped API keys to invoke org-scoped webhook operations. Attackers with app-scoped credentials can trigger signed outbound webhook deliveries for arbitrary organization webhooks outside their declared app boundary, bypassing the limited_to_apps authorization check. |
| CVE-2026-12396 | The WP Job Portal WordPress plugin before 2.5.5 does not perform capability or ownership checks before allowing job moderation actions, allowing authenticated users with a subscriber-level (self-registerable) account to approve, feature, or reject arbitrary jobs, including those owned by other users. |
| CVE-2026-56293 | Capgo before 12.128.2 contains an authorization flaw in transfer_app() that fails to update deploy_history.owner_org when transferring applications between organizations. Attackers can exploit this omission to retain unauthorized access to deployment history records in the source organization or cause the destination organization to lose access to transferred application deployment records. |
| CVE-2026-55808 | Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Drupal core allows Cross-Site Scripting (XSS). This issue affects Drupal core versions: from 0.0.0 to 10.5.12, from 10.6.0 to 10.6.11, from 11.2.0 to 11.2.14, from 11.3.0 to 11.3.12, from 0.0.0 to 11.0.*, from 0.0.0 to 11.1.*. |
| CVE-2026-10085 | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to restrict the group_constrained channel flag to public and private channels that support group synchronization, which allows an ordinary group or direct message member to remove all participants from the conversation via the channel patch API.. Mattermost Advisory ID: MMSA-2026-00688 |
| CVE-2026-61958 | Missing Authorization vulnerability in Saad Iqbal License Manager for WooCommerce license-manager-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects License Manager for WooCommerce: from n/a through <= 3.0.17. |
| CVE-2026-56359 | n8n before 2.8.0 contains a cross-site scripting vulnerability in the credential management flow where authenticated users can inject malicious JavaScript URLs into OAuth2 credential Authorization URL fields. Attackers can craft malicious credentials and trick victims into clicking the OAuth authorization button, executing arbitrary scripts in their browser session with the victim's privileges. |
| CVE-2026-55432 | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, the `CreateSubAgent` RPC did not validate a requested app sharing level against the template's `MaxPortSharingLevel` before persisting workspace apps, letting a workspace owner exceed the administrator's configured maximum. Exploitation requires the ability to register sub-agent apps in a workspace the attacker controls. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2clamps the sub-agent app sharing level to the template's `MaxPortSharingLevel`. As a workaround, disable wildcard app hostnames (`CODER_WILDCARD_ACCESS_URL`) to block subdomain-based app routing. |
| CVE-2026-9597 | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4 fail to verify whether a guest account is deactivated before creating a session in the magic-link token login path, which allows a deactivated guest user to obtain a fully functional session via a magic-link token issued prior to deactivation.. Mattermost Advisory ID: MMSA-2026-00681 |
| CVE-2026-55437 | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.17, 2.32.7, 2.33.8, and 2.34.2, the `AgentLogLine` dashboard component instantiated `ansi-to-html` without `escapeXML: true` and inserted the result via `dangerouslySetInnerHTML` so HTML embedded in workspace agent log lines was rendered as live markup. Server-side sanitization did not neutralize HTML metacharacters. Exploitation requires a victim to view attacker-controlled agent logs in the dashboard. The fix in versions 2.29.17, 2.32.7, 2.33.8, and 2.34.2 enables `escapeXML: true` so HTML metacharacters are escaped before DOM insertion. No known workarounds are available. |
| CVE-2026-56775 | n8n before 1.123.55, 2.25.7, and 2.26.2 contains an authorization vulnerability in three mutating evaluation test-run endpoints that authorize state-changing actions using the workflow:read scope instead of the action-appropriate workflow:execute scope. On instances using Advanced Permissions (Enterprise/Cloud) with projects and viewer roles, an authenticated user with the project:viewer role can start new evaluation test runs, cancel in-flight runs, and delete run records for workflows they only have read access to. |
| CVE-2026-55433 | Coder allows organizations to provision remote development environments via Terraform. Prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, the devcontainer recreate endpoint relied on route middleware that checked only `ActionRead` on the workspace and, unlike the sibling delete endpoint, performed no `ActionUpdate` check before triggering the destructive rebuild. Exploitation requires an existing low-privilege role with access to the target workspace. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 adds an explicit `ActionUpdate` authorization check before the agent is dialed like the delete endpoint. No known workarounds are available. |
| CVE-2026-15669 | A vulnerability was found in louisho5 picobot up to 0.2.0. This issue affects the function ExecTool.Execute of the file internal/agent/tools/exec.go of the component exec Tool. The manipulation results in os command injection. The attack requires a local approach. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-8384 | In Eclipse Jetty, an HTTP URI of this form: /public;/../admin/secret.txt results in an unresolved path of: /public/../admin/secret.txt instead of the expected: /admin/secret.txt Jetty itself is not affected, as it will not serve the secret.txt file because it will not pass the alias checker (only resolved resources are served). However, web applications that rely on resolved paths being provided by Jetty may be confused when receiving an unresolved path. |
| CVE-2026-6790 | In Eclipse Jetty, for HTTP/1, HTTP/2 and HTTP/3 requests, there is no strict check that the request authority (host and port) matches what provided in the Host header (if present). This was not enforced in earlier HTTP RFC (for example, in RFC 2616), but it is in the latest RFC (9110 and 9112). This mismatch can cause a number of problems that may be classified as vulnerabilities such as: * URI constructions (for example, for redirects -- this is typical for login pages) * Virtual host selection * Reverse proxying * Misleading logs * Etc. Given that the latest RFCs require that request authority and Host header must match, Jetty should enforce this invariant. |
| CVE-2026-15182 | A vulnerability has been found in GNU LibreDWG up to 0.13.4. The affected element is the function dwg_bmp of the file src/dwg.c of the component BMP Image Handler. Such manipulation leads to heap-based buffer overflow. The attack must be carried out locally. The exploit has been disclosed to the public and may be used. Upgrading to version 0.14 is sufficient to fix this issue. The name of the patch is 18fd542bb4d5ccedf9de12052bf50068b2b26f06. It is suggested to upgrade the affected component. |
| CVE-2026-15204 | A vulnerability was detected in TOTOLINK X5000R 9.1.0cu.2415_B20250515/9.1.0cu.2350_B20230313. Affected by this vulnerability is the function exportOvpn of the file /web/cgi-bin/cstecgi.cgi of the component OpenVPN Export. The manipulation results in path traversal. The attack may be launched remotely. |
| CVE-2026-12606 | Eclipse Grizzly in versions before 5.0.2, cannot properly parse the trailer section in malformed trailer header's line, which can be leveraged to perform HTTP request smuggling. |
| CVE-2026-61454 | The Grav Admin2 plugin (getgrav/grav-plugin-admin2) before 2.0.4 embeds a global JavaScript variable window.__GRAV_CONFIG__ in the Admin2 SPA bootstrap page at /grav/admin (and its subroutes). This object is returned in every unauthenticated response and discloses the server URL, API prefix, admin base path, runtime environment type, and exact Grav and Admin2 version numbers, allowing an unauthenticated attacker to fingerprint the deployment and select version-specific exploits without reconnaissance. |

| | |
|---|---|
| CVE-2026-59218 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.10.0, the /api/v1/auths/signin endpoint looked users up by email and only ran bcrypt password verification when a credential existed, making registered-account attempts measurably slower than missing-email attempts and allowing unauthenticated account enumeration. This issue is fixed in version 0.10.0. |
| CVE-2026-15193 | A vulnerability was determined in AidanPark openclaw-android up to 0.4.0. The affected element is an unknown function of the file android/app/src/main/java/com/openclaw/android/JsBridge.kt of the component Android WebView Bridge. This manipulation causes os command injection. The attack can only be executed locally. The exploit has been publicly disclosed and may be utilized. The pull request to fix this issue awaits acceptance. |
| CVE-2026-56284 | Capgo (Cap-go/capgo) before 12.128.2 contains an information disclosure vulnerability in the Supabase PostgREST RPC function public.get_total_metrics(org_id), which is callable by the anon role using only the public sb_publishable_* key. An unauthenticated attacker can probe organization existence and leak sensitive usage metrics including MAU, bandwidth, and install counts by sending POST requests to /rest/v1/rpc/get_total_metrics with valid organization UUIDs. |
| CVE-2026-9028 | The CorvusPay WooCommerce Payment Gateway plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.7.4. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to cancel any WooCommerce order placed via the CorvusPay payment method by supplying an arbitrary order number to the /wp-json/corvuspay/cancel/ REST endpoint. |
| CVE-2026-8609 | An unauthenticated attacker can repeatedly call Grafana's OAuth login route with unique values, causing unbounded memory growth that can eventually exhaust memory and crash the Grafana instance (denial of service). |
| CVE-2026-9017 | The NEX-Forms – Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 9.2.2. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to overwrite the saved_admin_email, saved_user_email, and saved_user_email_address fields of arbitrary form entries belonging to other users, and cause the site to dispatch attacker-controlled email content to attacker-chosen recipient addresses. |
| CVE-2026-9027 | The CorvusPay WooCommerce Payment Gateway plugin for WordPress is vulnerable to Payment Bypass via Improper Verification of Cryptographic Signature in all versions up to, and including, 2.7.4. The `corvuspay_success_handler` function registers the REST endpoint `POST /wp-json/corvuspay/success/` with `'permission_callback' => '__return_true'`, and while it calls `$this->client->validate->signature()` and stores the boolean result in `$res`, the result is never evaluated in a conditional — it is only written to the debug log — causing execution to unconditionally reach `$order->payment_complete()` regardless of whether the cryptographic signature is valid. This makes it possible for unauthenticated attackers to mark any pending WooCommerce order as fully paid by sending a POST request to the success endpoint containing an arbitrary or forged signature value, allowing them to obtain goods or services without payment. Because WooCommerce order IDs are sequential integers, target orders are trivially enumerable via the `order_number` POST parameter, requiring no prior knowledge of the victim order. |
| CVE-2026-13450 | The GamiPress – Gamification plugin to reward points, achievements, badges & ranks in WordPress plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 7.9.4 via the 'access' parameter due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to view private GamiPress activity log entries belonging to any user, including badge earnings, points balance changes, and event records from integrated plugins such as WooCommerce, LearnDash, and BuddyPress. This is exploitable by any unauthenticated visitor because the required 'gamipress' nonce is broadcast to all front-end users via wp_localize_script on the wp_enqueue_scripts hook, making the sole authentication barrier trivially bypassable. |
| CVE-2026-57474 | Deloitte AI Assist for Customer disclosed some configuration information through public-facing API endpoints that accepted unauthenticated requests. This information could reduce an attacker’s reconnaissance effort. On 2026-03-25, AI Assist for Customer restricted network access and enforced authentication for the previously exposed endpoints. |
| CVE-2026-11875 | The WP Support Plus Responsive Ticket System WordPress plugin through 9.1.2 does not sign or verify its guest-session cookie, allowing unauthenticated attackers to forge it and impersonate any ticket owner (identified by email address) to read, reply to, and close that person's support tickets. |
| CVE-2026-12516 | The Fediverse Embeds WordPress plugin before 1.5.8 does not validate the destination of the server-side request performed by an unauthenticated media-proxying endpoint, allowing anonymous users to make the site fetch arbitrary URLs, including internal and private-network addresses, and read back the response body. This results in a full-read Server-Side Request Forgery and open proxy. |
| CVE-2026-12517 | The Fediverse Embeds WordPress plugin before 1.5.8 does not validate the destination of the server-side request performed by an unauthenticated site-info endpoint before fetching it, allowing anonymous users (the gating nonce is exposed on public pages carrying an embed) to make the site request internal and private-network URLs and read back the parsed page metadata. This is a Server-Side Request Forgery. |
| CVE-2026-15621 | A vulnerability was detected in mosaxiv clawlet up to 0.2.10. This impacts the function read_file/write_file/edit_file of the file tools/fs_ops.go of the component File Tools. Performing a manipulation results in link following. The attack needs to be approached locally. The reported GitHub issue was closed with the label "not planned". |
| CVE-2026-12406 | The User Frontend: AI Powered Frontend Posting, User Directory, Profile, Membership & User Registration plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.3.7. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to delete arbitrary media attachments whose post_author is 0, such as guest and registration-form uploads, via the wpuf_file_del AJAX action. This is exploitable by unauthenticated visitors on any site where a WPUF shortcode is rendered on a front-end page, as this causes the valid wpuf_nonce value to be localized into publicly accessible JavaScript objects (wpuf_upload and wpuf_frontend), satisfying the sole access control gate. |
| CVE-2026-12418 | The User Frontend: AI Powered Frontend Posting, User Directory, Profile, Membership & User Registration plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.3.7 via the 'wpuf_files_data' parameter due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to overwrite the post_title, post_content, and post_excerpt of any arbitrary post on the site, including posts authored by administrators. Exploitation requires access to any WPUF post submission form; this is achievable by users with no WordPress role, as the wpuf_submit_post AJAX action is gated only by a nonce with no capability check for the downstream post-edit operation. |
| CVE-2026-12994 | The WCFM – Frontend Manager for WooCommerce plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 6.7.27. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to inject arbitrary reply content into any store inquiry, overwrite the main inquiry record in wp_wcfm_enquiries, and trigger unsolicited notification emails to customers and vendors. Unlike sibling controller branches (wcfm-enquiry and wcfm-enquiry-manage), the wcfm-my-account-enquiry-manage branch performs no is_user_logged_in() or current_user_can() check, and the nonce that serves as the sole barrier is embedded into every public page load without any login gate. |
| CVE-2026-9021 | The Easy Invoice plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 2.1.19. This is due to the plugin registering the easy_invoice_accept_quote and easy_invoice_decline_quote AJAX actions via wp_ajax_nopriv_ hooks and relying solely on a quote-scoped nonce that is rendered into the publicly accessible single quote template, combined with an ownership check that is gated behind an off-by-default Pro option (easy_invoice_pro_restrict_quote_to_client). This makes it possible for unauthenticated attackers to accept or decline arbitrary published quotes — and, depending on the configured accept action, automatically convert them into invoices (and even email them to the client) — by harvesting the per-quote nonce from the public quote page and submitting it to admin-ajax. |
| CVE- | The Context Blog theme for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.3.5 via the |

| | |
|---|---|
| 2026-6801 | context_blog_modal_popup. This makes it possible for unauthenticated attackers to extract the content of password-protected posts. |
| CVE-2026-31983 | A Missing Authentication vulnerability was discovered in the SSH keys synchronization endpoint. An unauthenticated attacker can send a request to the SSH keys synchronization endpoint and obtain the list of users that have uploaded their public SSH keys, their groups, and the uploaded public SSH keys. |
| CVE-2026-7558 | The Age Verification & Identity Verification by Token of Trust plugin for WordPress is vulnerable to unauthorized access in all versions up to and including 4.0.2. This is due to the handle_export_table() function being registered on the WordPress 'init' hook, which fires for all requests, including those from unauthenticated visitors, without any capability check. This makes it possible for unauthenticated attackers to download a CSV file containing sensitive WooCommerce donation data, including order dates, order IDs, charitable donation amounts, and admin-only order edit URLs, simply by visiting any page on the site with the 'tot_export_table' GET parameter set to a numeric value (0–3). |
| CVE-2026-11802 | The FoodBook Lite - Online Food Ordering System plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.5.6. The registration() function, accessible via the wp_ajax_nopriv_registration_action AJAX action, lacks any nonce verification or capability check, and does not check the WordPress users_can_register option before calling wp_insert_user(). This makes it possible for unauthenticated attackers to create new user accounts with the 'customer' role and receive authentication cookies, even when the site administrator has explicitly disabled user registration. |
| CVE-2026-15622 | A flaw has been found in poco-ai poco-claw up to 0.5.4. Affected is the function get_workspace_file of the file executor_manager/app/api/v1/workspace.py of the component Workspace API. Executing a manipulation of the argument user_id can lead to authorization bypass. The attack may be launched remotely. The exploit has been published and may be used. This patch is called 67fcc88505c57f77d3fcf04eb5b89425b10cbf48. Upgrading the affected component is recommended. |
| CVE-2026-61985 | Missing Authorization vulnerability in magepeopleteam Car Rental Manager car-rental-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Car Rental Manager: from n/a through <= 1.3.7. |
| CVE-2026-56296 | Cap-go before 12.128.2 contains an information disclosure vulnerability in the public.transfer_app RPC function that returns distinct error messages for existing versus non-existing app IDs. Unauthenticated attackers can enumerate valid app IDs by observing error message differences when calling transfer_app with only the publishable API key. |
| CVE-2026-59817 | Ghost is a Node.js content management system. From 6.27.0 before 6.44.0, Ghost's public donation checkout flow allowed an unauthenticated attacker to control donation checkout metadata and obtain full paid gift memberships for a minimal payment without exposing customer or member data or stealing money from a site or its members. This issue is fixed in version 6.44.0. |
| CVE-2026-61983 | Missing Authorization vulnerability in andy_moyle Church Admin church-admin allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Church Admin: from n/a through <= 5.0.30. |
| CVE-2026-61344 | The Superior Court of California Hearing Reminder Service at https://www.hrs.courts.ca.gov exposes an API endpoint that returns court reminder records containing potentially sensitive information without authentication. |
| CVE-2026-50415 | Exposure of sensitive information to an unauthorized actor in Windows Media allows an unauthorized attacker to disclose information over a network. |
| CVE-2026-54470 | Dell Unisphere for PowerMax, version(s) 10.3.0.5 and prior contain(s) an Improper Restriction of XML External Entity Reference vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access. |
| CVE-2026-15553 | Enterprise Cloud Database developed by Ragic has a Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload malicious files and make them available for users to download. |
| CVE-2026-15530 | A flaw has been found in WuzhiCMS up to 4.1.0. Affected by this vulnerability is the function config/listimage of the file /index.php?m=attachment&f=index&v=upload of the component Attachment API. Executing a manipulation can lead to information disclosure. The attack can be launched remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-59828 | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, post revisions that should be hidden from regular users could be leaked through visible diffs on adjacent revisions serialized by PostRevisionSerializer. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5. |
| CVE-2026-44342 | New API is a large language mode (LLM) gateway and artificial intelligence (AI) asset management system. Prior to 0.12.0-alpha.1, the email and WeChat account binding endpoints GET /api/oauth/email/bind and GET /api/oauth/wechat/bind used GET requests for state-changing account operations, allowing an attacker to trigger a logged-in user's browser to bind an attacker-controlled email address or OAuth identity in deployments where session cookies could be sent on cross-site navigations. This issue is fixed in version 0.12.0-alpha.1. |
| CVE-2026-15531 | A vulnerability has been found in yashbhalgat HashNeRF-pytorch up to 82885e698295982504eb6a26d060a6b2473e3706. Affected by this issue is the function torch.load of the file run_nerf.py of the component Checkpoint File Handler. The manipulation of the argument ckpt_path leads to deserialization. The attack must be carried out locally. The exploit has been disclosed to the public and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The pull request to fix this issue awaits acceptance. |
| CVE-2026-14500 | The Bulk Order Update for WooCommerce plugin for WordPress is vulnerable to Arbitrary File Read in versions up to, and including, 1.6. This is due to the bouw_fetch_csv_data() AJAX handler being registered on the wp_ajax_nopriv_ hook with no capability or nonce check, and passing the attacker-supplied csv_url POST parameter — filtered only by esc_url_raw() (which leaves absolute filesystem paths intact) and validate_file() (which only rejects '..' traversal patterns) — directly into fopen()/fgetcsv() and reflecting the first parsed line in the JSON response. This makes it possible for unauthenticated attackers to read the first line of arbitrary files on the server (such as /etc/passwd) and to use the handler as a file-existence oracle. |
| CVE-2026-15302 | The ARMember plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 4.0.27 via the 'X-FILENAME' HTTP header. This makes it possible for unauthenticated attackers to upload and overwrite certain files (e.g., CSS) to directories outside the 'wp-content/uploads/armember' directory. |
| CVE-2026-12097 | The User Management plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.2. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to modify the plugin's export field configuration stored in the uiewp_export_field option, controlling which user fields such as password hashes are included in CSV exports and how columns are mapped during imports. |
| CVE- | |

| | |
|---|---|
| 2026-44806 | Missing release of memory after effective lifetime in Windows Cryptographic Services allows an unauthorized attacker to deny service over a network. |
| CVE-2026-11990 | The KiviCare – Clinic & Patient Management System (EHR) plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.4.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to mark arbitrary pending appointments as Confirmed and forge an associated completed payment record in wp_kc_payments_appointment_mappings using an attacker-supplied payment ID, bypassing payment entirely. This exploit is achievable on a default installation because the gateway resolution logic returns all registered gateways regardless of admin-enabled status, making the manual (KCPayLater) gateway always selectable. |
| CVE-2026-6802 | The Easy Upload Files During Checkout plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 3.0.1. This is due to missing authorization checks in the ufdc_custom_init() function, which processes the 'eufdc-delete' parameter without any nonce verification, capability check, or attachment ownership validation. This makes it possible for unauthenticated attackers to permanently delete arbitrary media library attachments from the WordPress site. |
| CVE-2026-12276 | The LA-Studio Element Kit for Elementor WordPress plugin before 1.6.1 does not check whether user registration is enabled on the site before creating an account through one of its unauthenticated AJAX actions, allowing unauthenticated attackers to register new accounts even when registration has been disabled site-wide. |
| CVE-2026-59203 | Pillow is a Python imaging library. From 12.0.0 through 12.2.0, Pillow's EPS parser in PIL/EpsImagePlugin.py accepts a negative byte count in the %%BeginBinary directive, allowing a crafted EPS file to cause Image.open() to seek backwards to the same directive and parse it repeatedly in an infinite loop. This issue is fixed in version 12.3.0. |
| CVE-2026-60118 | Hi.Events before 1.11.0 contains a missing server-side visibility enforcement vulnerability that allows unauthenticated attackers to purchase hidden tickets by referencing hidden product and price IDs in order creation requests without authorization checks. Attackers can enumerate sequential hidden ticket IDs from visible ones and submit order creation requests referencing those IDs to purchase VIP, invite-only, or discounted tickets intentionally withheld from public sale. |
| CVE-2026-50432 | Use after free in Windows Virtual Filtering Platform (VFP) allows an authorized attacker to deny service over a network. |
| CVE-2026-57029 | A Missing Synchronization vulnerability in the flow collector handler of Juniper Networks Junos OS Evolved on QFX Series allows an adjacent, unauthenticated attacker to cause a Denial-of-Service (DoS). When the reachability of an sFlow collector changes, the corresponding next-hop entry is updated. If this update occurs simultaneously with the sFlow thread accessing the next-hop data (which is outside the attackers control), it causes the evo-pfemand process to crash, impacting all traffic forwarding until the automatic process restart has completed. This issue affects Junos OS Evolved on QFX Series: * all 23.2 versions, * 23.4 versions before 23.4R2-S7-EVO, * 24.2 versions before 24.2R2-S5-EVO, * 24.4 versions before 24.4R2-S3-EVO, * 25.2 versions before 25.2R2-EVO. |
| CVE-2026-15527 | A vulnerability has been found in better-auth better-icons up to 1.0.5. This vulnerability affects unknown code of the component scan_project_icons/sync_icon. Such manipulation of the argument icons_file leads to path traversal. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-56336 | Capgo before 12.128.2 contains an information disclosure vulnerability in the unauthenticated /private/sso/check-domain endpoint that returns internal org_id and provider_id values. Attackers can enumerate email domains to build mappings of domains to organization UUIDs and SSO provider identifiers, enabling reconnaissance against Capgo tenants. |
| CVE-2026-15035 | A vulnerability was found in bentoml OpenLLM 0.6.30. This affects the function async_run_command of the file src/openllm/common.py of the component Model Repository Directory Name Handler. Performing a manipulation of the argument cmd results in command injection. Attacking locally is a requirement. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-15475 | A weakness has been identified in MiniTool Partition Wizard up to 13.6. The affected element is an unknown function in the library pwdrvio.sys of the component Signed Kernel Driver. This manipulation causes improper access controls. The attack can only be executed locally. The exploit has been made available to the public and could be used for attacks. Upgrading to version 13.9 is sufficient to fix this issue. The affected component should be upgraded. The vendor was contacted early about this disclosure. |
| CVE-2026-60086 | PraisonAI before 4.6.78 contains a prompt injection defense bypass vulnerability where the injection defense only blocks threats classified as CRITICAL, requiring three or more detector families to match simultaneously. Attackers can craft single or double-vector prompt injections that are classified as HIGH threat level and pass through unblocked to reach the model. |
| CVE-2026-15476 | A security vulnerability has been detected in QILING Disk Master 6.0.0.0. The impacted element is an unknown function in the library diskbckp.sys of the component Kernel Driver. Such manipulation leads to improper access controls. The attack can only be performed from a local environment. The exploit has been disclosed publicly and may be used. It is suggested to upgrade the affected component. |
| CVE-2026-11869 | The WP DSGVO Tools (GDPR) WordPress plugin before 3.1.40 does not perform an authorization check on the immediate-processing path of its data subject access request feature, allowing unauthenticated attackers to generate and download the full personal-data export (including name, postal address, phone number, email, and comment content) of any user, customer, or commenter by supplying their email address. |
| CVE-2026-5459 | The User Frontend: AI Powered Frontend Posting, User Directory, Profile, Membership & User Registration plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.3.1 via the payment_page() function due to missing validation on the 'user_id' user controlled key. This makes it possible for unauthenticated attackers to activate a free subscription pack for any user on the site, overwriting their existing paid subscription and causing loss of paid features. |
| CVE-2026-45780 | Discourse is an open-source discussion platform. Prior to 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5, EventSerializer could expose invited group names, sample invitees, and attendance statistics to users who could view the topic but were not entitled to view the private event invitee list. This issue is fixed in versions 2026.6.0, 2026.5.1, 2026.4.2, and 2026.1.5. |
| CVE-2026-15522 | A security flaw has been discovered in tugcantopaloglu godot-mcp 2.0.0. Affected by this vulnerability is the function validatePath of the file build/index.js of the component run_project. The manipulation of the argument projectPath results in path traversal. Attacking locally is a requirement. The exploit has been released to the public and may be used for attacks. Upgrading to version 3.0.0 addresses this issue. The patch is identified as eb63add552aa4bd9205395cf91b40654654a3cf2. It is suggested to upgrade the affected component. |
| CVE-2026-57994 | phpMyFAQ before 4.1.5 applies inconsistent active=yes and publication-date filtering across its public FAQ API endpoints, allowing unauthenticated attackers to retrieve inactive (draft or review-only) FAQ content. Specifically, GET /api/v3.1/faq/{categoryId}/{faqId} returns the inactive FAQ title and full answer, while GET /api/v3.1/faqs/tags/{tagId} and GET /api/v4.0/faqs/tags/{tagId} return the inactive FAQ title and answer preview, disclosing non-public content. |
| CVE-2026- | DeepSeek MCP Server is an MCP server for DeepSeek V4. Starting in version 1.4.2 and prior to version 1.8.0, the self-hosted HTTP transport of `@arikusi/deepseek-mcp-server` exposes `POST /mcp` without any authentication: `createMcpExpressApp` is called without an `authProvider` and no middleware guards the route, so any network-reachable client can issue an unauthenticated `initialize` request and obtain a valid MCP session identifier. In reproduced testing against commit `5e1302171e99`, an unauthenticated client was able to initialize a session, enumerate tools, and invoke the local `deepseek_sessions` tool with |

| | |
|---|---|
| 55605 | no credentials. The same unauthenticated session also exposes `deepseek_chat`, whose handler uses the server-side `DEEPSEEK_API_KEY` when self-hosted deployments configure one. This issue applies to self-hosted HTTP mode, not the separately documented hosted BYOK endpoint in `README.md`, which expects an `Authorization: Bearer ...` header. Upstream self-hosted container assets enable HTTP mode by default (`Dockerfile`) and publish port `3000` (`docker-compose.yml`). Version 1.8.0 contains a patch for this issue. |
| CVE-2026-57021 | An Out-of-bounds Write vulnerability in the http-gatekeeper (http-gk) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). If an SRX Series device is configured for remote-access VPN with pre-logon compliance check, a network-based attacker sending specifically formatted requests can trigger an out of bounds write leading to an http-gk process crash. This crash leads to unavailability of all services depending on the [ system services web-management ] configuration (like J-Web, remote access VPN and firewall authentication) until the process automatically restarts. This issue affects Junos OS on SRX Series: * 23.2 versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S4, * 25.2 versions before 25.2R2, * 25.4 versions before 25.4R1-S1, 25.4R2. |
| CVE-2026-15520 | A vulnerability was determined in GNU LibreDWG 0.13.4-154-g0b573035. This impacts the function decompress_R2004_section of the file src/decode.c of the component R2004 Section Decompression. Executing a manipulation can lead to heap-based buffer overflow. The attack requires local access. The exploit has been publicly disclosed and may be utilized. Upgrading to version 0.14.8396 will fix this issue. This patch is called 3d0f9fc2eddbd6579c99af3111c37c98f03475d0. You should upgrade the affected component. |
| CVE-2026-57024 | A Use of Multiple Resources with Duplicate Identifier vulnerability in the IKE daemon (iked) of Juniper Networks Junos OS on MX with SPC3 and SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). On an MX with SPC3 and SRX devices configured for VPN service, when a large number of VPN negotiations fail a peer index rollover will eventually occur. As a result, new peers are assigned index values that are already in use and the iked process starts to crash repeatedly. This results in failure to establish new VPN connections and rekeying existing ones. To restore service the system must be rebooted. Please note that the index value can't be monitored, so customers should monitor tunnel up and down events and if a lot of events occur over an extended period of time it becomes likely that this issue occurs. To be exposed to this issue the system needs to run iked (vs. kmd which is not affected), which can be verified with: user@host> show system processes extensive \| match "KMD\|IKED" This issue affects Junos OS on MX with SPC3, SRX Series: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S6, * 24.2 versions before 24.2R2-S3, * 24.4 versions before 24.4R2-S4, * 25.2 versions before 25.2R1-S1. |
| CVE-2026-15521 | A vulnerability was identified in makafeli n8n-workflow-builder up to 0.11.0. Affected is an unknown function of the file build/server.cjs of the component update_node_from_file. The manipulation of the argument filePath leads to path traversal. An attack has to be approached locally. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-57475 | Deloitte AI Assist for Customer accepted unauthenticated POST requests through public-facing API endpoints that allowed a remote attacker to make limited additions to the configuration. These additions were not used by the system. On 2026-03-25, AI Assist for Customer restricted network access and enforced authentication for the previously exposed endpoints. |
| CVE-2026-56164 | Missing authentication for critical function in Microsoft Office SharePoint allows an unauthorized attacker to elevate privileges over a network. |
| CVE-2026-61977 | Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Crocoblock JetSearch jet-search allows Retrieve Embedded Sensitive Data.This issue affects JetSearch: from n/a through <= 3.6.1.2. |
| CVE-2026-57776 | Missing Authorization vulnerability in vowelweb VW Wedding vw-wedding allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects VW Wedding: from n/a through <= 1.3.7. |
| CVE-2026-61975 | Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Crocoblock JetReviews jet-reviews allows Retrieve Embedded Sensitive Data.This issue affects JetReviews: from n/a through <= 3.0.1. |
| CVE-2026-13039 | The Eventin – Event Calendar, Event Registration, Tickets & Booking (AI Powered) plugin for WordPress is vulnerable to authorization bypass due to a regression in versions from 4.0.26 up to and including 4.1.15. This is due to the plugin not properly verifying that a user is authorized to perform an action in the payment_complete() function of PaymentController.php. This makes it possible for unauthenticated attackers to mark unpaid ticket orders as completed by submitting a fabricated SureCart checkout ID or FluentCart cart hash, granting themselves paid event access, QR-code attendee tickets, and order confirmation emails without making any real payment. The wp_rest nonce required to reach the vulnerable endpoint is embedded in every public event page, meaning no WordPress session or credentials are needed to obtain it. This vulnerability represents a regression — the same function and endpoint were previously patched but the fix did not persist through subsequent releases. |
| CVE-2026-59870 | js-yaml is a JavaScript YAML parser and dumper. From 5.0.0 before 5.2.1, YAML11_SCHEMA support for the !!omap tag in src/tag/sequence/omap.ts uses omapTag.addItem() to perform a linear duplicate-key scan on every insertion, causing O(n^2) CPU consumption when yaml.load() parses a crafted ordered-map document. This issue is fixed in version 5.2.1. |
| CVE-2026-59927 | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, the Include directive in src/mistune/directives/include.py detects only direct self-includes and not indirect cycles, allowing two markdown files that include each other to trigger unbounded recursion, raise RecursionError, and crash the rendering request. This issue is fixed in version 3.3.0. |
| CVE-2026-57774 | Missing Authorization vulnerability in vowelweb VW Food Corner vw-food-corner allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects VW Food Corner: from n/a through <= 1.1.0. |
| CVE-2026-59868 | js-yaml is a JavaScript YAML parser and dumper. From 5.0.0 before 5.2.0, when merge keys are enabled, js-yaml can spend quadratic CPU time parsing a document whose size grows only linearly when a chain of mappings uses merge keys where each mapping merges the previous one. This issue is fixed in version 5.2.0. |
| CVE-2026-44332 | Fiber is an Express inspired web framework written in Go. Prior to 3.3.0, the default Authorizer function in the BasicAuth middleware in middleware/basicauth/config.go uses short-circuit evaluation that skips password hash comparison for non-existent usernames, enabling reliable remote username enumeration through response timing differences. This issue is fixed in version 3.3.0. |
| CVE-2026-59875 | node-tar is a tar archive manipulation library for Node.js. Prior to 7.5.17, node-tar does not strip NUL bytes from PAX path and linkpath records in src/pax.ts, allowing a crafted archive with values to reach fs.lstat or fs.open and terminate the process with an uncaught exception. This issue is fixed in version 7.5.17. |
| CVE-2026-57778 | Missing Authorization vulnerability in wpdevart Booking calendar, Appointment Booking System booking-calendar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Booking calendar, Appointment Booking System: from n/a through <= 3.2.36. |
| CVE-2026- | The Members – Membership & User Role Editor Plugin plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.2.22 via the members_filter_protected_posts_for_rest. This makes it possible for unauthenticated attackers to extract determine the existence and exact count |

| | |
|---|---|
| 12426 | of access-restricted posts, and use per-page pagination as a boolean oracle to infer keywords and content contained within those hidden restricted posts. |
| CVE-2026-61976 | Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Crocoblock JetBlocks For Elementor jet-blocks allows Retrieve Embedded Sensitive Data.This issue affects JetBlocks For Elementor: from n/a through <= 1.5.0. |
| CVE-2026-57779 | Missing Authorization vulnerability in themebeez Fascinate fascinate allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fascinate: from n/a through <= 1.1.5. |
| CVE-2026-57782 | Missing Authorization vulnerability in PressTigers Universal Clocks universal-clocks allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Universal Clocks: from n/a through <= 1.2.0. |
| CVE-2026-42505 | Handshakes which used Encrypted Client Hello could be de-anonymized by a passive network observer due to a disclosure of pre-shared key identities in the unencrypted client hello. |
| CVE-2026-59871 | node-tar is a tar archive manipulation library for Node.js. Prior to 7.5.18, node-tar coerces all-digit PAX path and linkpath values in src/pax.ts to JavaScript numbers, causing downstream path handling such as normalizeWindowsPath(entry.path).split('/') to throw an uncaught TypeError. This issue is fixed in version 7.5.18. |
| CVE-2026-57781 | Missing Authorization vulnerability in Sovlix MeetingHub meetinghub allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MeetingHub: from n/a through <= 1.25.10. |
| CVE-2026-59877 | protobufjs compiles protobuf definitions into JavaScript (JS) functions. Prior to 7.6.5 and 8.6.6, protobufjs parsed option names by advancing through schema tokens until reaching an = token without checking for end of input, so a crafted .proto schema that opens an option declaration and ends prematurely can cause parse, Root.load, or Root.loadSync to loop indefinitely. This issue is fixed in versions 7.6.5 and 8.6.6. |
| CVE-2026-29007 | U-Boot through 2026.04-rc3 contains an out-of-bounds read vulnerability in tcp_rx_state_machine() (net/tcp.c) when CONFIG_PROT_TCP is enabled, allowing remote attackers to read beyond TCP segment boundaries by crafting a malicious packet with a mismatched IP total length and TCP data offset field. Attackers can send a packet with an IP total length of 40 bytes and a TCP data offset claiming 60 bytes of header to cause tcp_parse_options() to read 40 bytes past the end of the TCP segment, potentially corrupting connection state variables such as rmt_win_scale and rmt_timestamp to disrupt TCP window calculations. |
| CVE-2026-59938 | pypdf is a free and open-source pure-python PDF library. Prior to 6.14.0, an attacker can craft a PDF with declared image size values that are much too large compared to the actual data, causing large memory usage in pypdf image parsing. This issue is fixed in version 6.14.0. |
| CVE-2026-61505 | Rejetto HFS 3.0.0 through 3.2.0 allows path traversal through the lang query parameter, permitting a remote unauthenticated attacker to read certain JSON files outside the shared folders. Exploitation is constrained to files matching a narrow naming and format pattern, limiting practical impact. |
| CVE-2026-13250 | The Solace Extra plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.5.3. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to permanently delete all content previously imported via the Starter Template feature, including posts, pages, media attachments, WooCommerce products, taxonomy terms, and sitebuilder templates. The required nonce is emitted on every wp-admin page via wp_localize_script() hooked to admin_enqueue_scripts without a page guard, meaning any Subscriber visiting /wp-admin/profile.php can obtain it; the handler is additionally registered via wp_ajax_nopriv_, making it reachable by fully unauthenticated users as well. |
| CVE-2026-6803 | The AI Chatbot & Workflow Automation by AIWU plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.4.12. This is due to missing capability checks and nonce verification on AJAX actions registered under both wp_ajax_ and wp_ajax_nopriv_ hooks, as the base controller's getPermissions() returns an empty array and neither removeGroup nor clear are added to getNoncedMethods(), causing the authorization gate to unconditionally return true for these actions. This makes it possible for unauthenticated attackers to delete specific records by ID or delete all records from any module's database table by unauthenticated attackers. |
| CVE-2026-61503 | Rejetto HFS 3.0.0 through 3.2.0 returns observably different responses from its login endpoint depending on whether the submitted username exists. A remote unauthenticated attacker can use this to confirm valid account names, including the default admin account, facilitating password-guessing and session-forgery attacks. |
| CVE-2026-6804 | The AI Chatbot & Workflow Automation by AIWU plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.4.12. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to publish draft WordPress posts, exposing unpublished content, or unpublish live content, causing service disruption, by supplying arbitrary scenario IDs. |
| CVE-2026-45045 | Fiber is an Express inspired web framework written in Go. Prior to 3.3.0 and 2.52.14, the BalancerForward proxy helper in middleware/proxy/proxy.go uses Header.Add() instead of Header.Set() when injecting X-Real-IP, allowing an attacker-supplied first X-Real-IP value to be forwarded to upstream servers for logging, rate limiting, and access control. This issue is fixed in version 3.3.0 and 2.52.14. |
| CVE-2026-11901 | The WP Hotel Booking plugin for WordPress is vulnerable to Insufficient Verification of Data Authenticity in all versions up to, and including, 2.3.1. This is due to the `web_hook_process_paypal_standard()` IPN handler selecting its PayPal validation endpoint from the attacker-controlled `$_REQUEST['test_ipn']` parameter, force-upgrading any `pending` transaction to `completed` when `test_ipn=1`, and omitting post-verification checks on `receiver_email`, `mc_currency`, and `txn_id` uniqueness after receiving a `VERIFIED` response from PayPal. This makes it possible for unauthenticated attackers to mark arbitrary hotel bookings as fully paid without submitting genuine payment to the merchant — either by routing IPN validation through PayPal's sandbox using a free sandbox account, or by replaying a previously verified IPN from a nominal payment to an attacker-controlled PayPal account. An attacker requires only a free PayPal sandbox account (or any PayPal account) to obtain a `VERIFIED` response; no site credentials or special configuration are needed. |
| CVE-2026-14906 | Pages with malicious titles could potentially allow saved PDF content to overwrite PDF files or bundled content within the Firefox for iOS application sandbox. This vulnerability was fixed in Firefox for iOS 152.4. |
| CVE-2026-10865 | The Cost Calculator Builder plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.0.11 via the (template body). This makes it possible for unauthenticated attackers to extract the plaintext Stripe secret key, Razorpay secret key, and PayPal client_secret embedded in the page source of any page containing a calculator, enabling full control of the merchant's payment gateway accounts. This exposure only occurs when the 'use in all calculators' option is enabled for one or more payment gateways in the plugin's global settings. |
| CVE-2026-50418 | Improper access control in Windows System allows an unauthorized attacker to bypass a security feature locally. |

| | |
|---|---|
| CVE-2026-57439 | CyberChef is a web app for encryption, encoding, compression, and data analysis. Prior to 11.2.0, the Series Chart operation accepts __proto__ as a key while parsing user-supplied CSV, allowing prototype pollution that can be chained with operations such as Parse UDP to inject malicious JavaScript into HTML output. This issue is fixed in version 11.2.0. |
| CVE-2026-15519 | A vulnerability was found in usestrix strix up to 1.0.2. This affects an unknown function of the file system_prompt.jinja of the component PyPI Handler. Performing a manipulation results in inclusion of functionality from untrusted control sphere. The attack is possible to be carried out remotely. The complexity of an attack is rather high. The exploitability is reported as difficult. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-57221 | RabbitMQ is a messaging and streaming broker. Prior to 3.13.15, 4.0.20, 4.1.11, and 4.2.6, RabbitMQ does not perform authorization checks on passive queue.declare and exchange.declare AMQP 0-9-1 operations, allowing any authenticated user who can connect to a virtual host to enumerate queue and exchange names and read queue message and consumer counts. This issue is fixed in versions 3.13.15, 4.0.20, 4.1.11, and 4.2.6. |
| CVE-2026-12081 | The Database for Contact Form 7, WPforms, Elementor forms WordPress plugin before 1.5.2 does not restrict the PHP classes allowed when unserializing an attacker-supplied form-field value, allowing unauthenticated users to inject arbitrary PHP objects that are instantiated when an administrator views the stored entry. This is an incomplete fix of CVE-2025-7384 and CVE-2026-2599, whose deserialization paths were hardened while the entry-editor file-field path was missed. |
| CVE-2026-59253 | n8n before 2.28.0 contains an improper authorization vulnerability allowing authenticated users to assign workflows to folders in other projects. Attackers can bypass project and folder authorization boundaries by supplying crafted request payloads during workflow creation, causing logical integrity violations in target project folder structures. |
| CVE-2026-55515 | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, the unaccepted-assets report delete endpoint authorizes only reports.view and deletes CheckoutAcceptance::pending()->find($acceptanceId) by global ID without checking access to the related checkoutable asset, allowing a reports user in one company to delete pending checkout acceptance records for another company. This issue is fixed in version 8.6.2. |
| CVE-2026-10664 | The nRF70 Wi-Fi driver's power-save event handler nrf_wifi_event_proc_get_power_save_info() in drivers/wifi/nrf_wifi/src/wifi_mgmt.c copied TWT (Target Wake Time) flow entries from an nrf_wifi_umac_event_power_save_info event into the fixed-size twt_flows[WIFI_MAX_TWT_FLOWS] (8-element) array of a caller-supplied struct wifi_ps_config, looping over event-provided num_twt_flows without validating it against WIFI_MAX_TWT_FLOWS or checking event_len. When num_twt_flows exceeds 8, the handler writes past the destination array (which is typically on the caller's stack, e.g. the wifi ps shell command) -- an out-of-bounds write of ~40-byte TWT entries -- and reads twt_flow_info[i] past the event buffer. The event is delivered by the nRF70 co-processor firmware in response to a host-initiated power-save GET, so reaching the overflow requires the firmware to emit a malformed or out-of-range event; the trust boundary is host-to-trusted-coprocessor rather than a direct remote-AP write, with over-the-air influence on the flow count being indirect and bounded by the 3-bit TWT flow-id space. Affected: builds with CONFIG_NRF70_STA_MODE on releases through v4.4.0. The fix rejects events with num_twt_flows > WIFI_MAX_TWT_FLOWS or with event_len shorter than the claimed entries, and adds a NULL check on the caller buffer. |
| CVE-2026-61970 | Server-Side Request Forgery (SSRF) vulnerability in Themeisle Auto Featured Image (Auto Post Thumbnail) auto-post-thumbnail allows Server Side Request Forgery.This issue affects Auto Featured Image (Auto Post Thumbnail): from n/a through <= 5.0.4. |
| CVE-2026-12918 | The Mail Mint – Email Marketing, Newsletter, Email Automation & WooCommerce Emails plugin for WordPress is vulnerable to generic SQL Injection via the 'recipients' parameter in all versions up to, and including, 1.24.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This is a second-order SQL injection: the malicious payload is first stored unsanitized via a POST request to /mrm/v1/campaigns/ (bypassing filter_recipients() validation because an int-cast of a string like '1) OR ...' evaluates to a real numeric ID), and is then triggered by a subsequent GET request to /mrm/v1/campaigns/{id} that deserializes the recipients and passes the raw id string through array_column() into the vulnerable query. |
| CVE-2026-12141 | The Premium Addons for Elementor – Powerful Elementor Templates & Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'premium_tooltip_text' parameter in all versions up to, and including, 4.11.84 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The injected payload is specifically triggered when an administrator or higher-privileged user opens the affected post in the Elementor editor, as the raw unescaped output occurs via the print_template() method registered on the 'elementor/section/print_template' hook rather than on the public-facing frontend. |
| CVE-2026-43752 | An authenticated administrator may be able to achieve arbitrary code execution on the host system by uploading a malicious file through the Open Source LLM setup feature in the Admin Console. This vulnerability has been addressed in FileMaker Server 26.0.1. |
| CVE-2026-55079 | Coder allows organizations to provision remote development environments via Terraform. Starting in version 2.24.0 and prior to versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2, `NewDataBuilder` in `provisionersdk/proto/dataupload.go` allocated a byte slice using the client-supplied `FileSize` from a `DataUpload` message without an upper-bound check. Although the DRPC wire limit is 4 MiB, the `FileSize` value itself was unconstrained. The fix in versions 2.29.7, 2.32.7, 2.33.8, and 2.34.2 validates `FileSize` against an upper bound (`MaxFileSize = 100 MiB`) before allocation. As a workaround, restrict access to the provisioner daemon serve endpoint to trusted provisioner daemon service accounts. |
| CVE-2026-12936 | The Recurio – Ultimate Subscription for WooCommerce plugin for WordPress is vulnerable to generic SQL Injection via the 'data' parameter in all versions up to, and including, 1.1.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with shop manager-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. |
| CVE-2026-62193 | OpenClaw versions 2026.6.5 before 2026.6.9 contain a vulnerability in the plugin install wrappers that could skip the install policy (authorization) check. When the affected feature is enabled and reachable, a lower-trust caller or a configured input path could execute or persist actions beyond the caller's intended authorization. Impact depends on the operator's configuration and whether lower-trust input can reach the affected path. The issue is fixed in 2026.6.9. |
| CVE-2026-9708 | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to validate that an assigned incoming webhook user has access to the target team or channel, which allows a requester with webhook management permissions to create posts or direct messages attributed to another user via crafted incoming webhook configuration and payloads.. Mattermost Advisory ID: MMSA-2026-00683 |
| CVE-2026-59854 | SiYuan is an open-source personal knowledge management system. Prior to 3.7.1, POST /api/file/globalCopyFiles accepts attacker-supplied absolute source paths and relies on util.IsSensitivePath in kernel/util/path.go, whose denylist misses common home-directory credential files such as .git-credentials, .netrc, .pgpass, .kube/config, .docker/config.json, and .gnupg, allowing an authenticated administrator or API-token user to copy those files into the workspace and exfiltrate them through the file API. This issue is fixed in versions 3.7.1-alpha.2 and 3.7.1. |
| CVE-2026-61952 | Missing Authorization vulnerability in Jose Vega WooCommerce Bulk Edit Products – WP Sheet Editor woo-bulk-edit-products allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WooCommerce Bulk Edit Products – WP Sheet Editor: from n/a through <= 1.8.21. |
| CVE- | LiteLLM is a proxy server (AI Gateway) to call LLM APIs in OpenAI (or native) format. Prior to 1.83.10-stable, LiteLLM's /health/test_connection endpoint resolved |

| | |
|---|---|
| 2026-59819 | request-supplied environment and OIDC file references in litellm_params, allowing a proxy administrator or another privileged caller with permission to test model connections to read files from the local filesystem via an oidc/file/ reference. This issue is fixed in version 1.83.10-stable. |
| CVE-2026-14475 | The Cookie Banner for GDPR / CCPA – WPLP Cookie Consent plugin for WordPress is vulnerable to generic SQL Injection via the 'scan_id' parameter in all versions up to, and including, 4.3.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. |
| CVE-2026-59193 | Grav is a file-based Web platform. Prior to 2.0.0, an authenticated admin.super user can crash Grav or fill the disk by uploading a specially crafted ZIP archive through the Direct Install tool because Installer::unZip calls ZipArchive::extractTo without limits on uncompressed size, entry count, or directory depth. This issue is fixed in version 2.0.0. |
| CVE-2026-14342 | The Mail Mint – Email Marketing, Newsletter, Email Automation & WooCommerce Emails plugin for WordPress is vulnerable to time-based SQL Injection via the 'contact_ids' parameter in all versions up to, and including, 1.24.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. |
| CVE-2026-0285 | A server-side request forgery (SSRF) vulnerability in Palo Alto Networks PAN-OS software enables an authenticated administrator with network access to the management web interface to make unauthorized requests from the firewall to internal services. The security risk posed by this issue is minimized when the management interface is restricted to only trusted internal IP addresses according to our recommended best practice deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . Panorama, Cloud NGFW, and Prisma® Access are not impacted by this vulnerability. |
| CVE-2026-11827 | GitLab has remediated an issue in GitLab EE affecting all versions from 9.5 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an authenticated user with maintainer-role permissions to obtain another user's stored credentials due to improper authorization controls. |
| CVE-2026-14362 | HashiCorp memberlist before version 0.6.0 is vulnerable to a denial-of-service issue in its push/pull state handling that may allow an attacker with network access to the gossip port to exhaust memory on a receiving node and cause the process to terminate. This vulnerability (CVE-2026-14362) is fixed in memberlist 0.6.0. |
| CVE-2025-5017 | The Catalyst Connect Zoho CRM Client Portal plugin for WordPress is vulnerable to time-based SQL Injection via the ‘uid’ parameter in all versions up to, and including, 2.2.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. |
| CVE-2026-57476 | Deloitte AI Assist for Customer exposed unauthenticated API endpoints that allowed an attacker with knowledge of additional parameters to read from or inject content into the retrieval-augmented generation (RAG) corpus. On 2026-03-25, AI Assist for Customer restricted network access and enforced authentication for the previously exposed endpoints. |
| CVE-2026-13243 | Cross-Site Request Forgery (CSRF) vulnerability in Drupal Salesforce Suite allows Cross Site Request Forgery. This issue affects Salesforce Suite versions: from 0.0.0 to 5.1.3. |
| CVE-2026-59876 | protobufjs compiles protobuf definitions into JavaScript (JS) functions. From 8.2.0 until 8.6.5, the protobufjs Text Format extension parsed string-keyed map entries using ordinary property assignment, allowing a map entry with key __proto__ to change the prototype of the returned map object instead of creating an own map entry in protobufjs/ext/textformat. This issue is fixed in version 8.6.5. |
| CVE-2026-13237 | Incorrect Authorization vulnerability in Drupal AI Agents allows Forceful Browsing. This issue affects AI Agents versions: from 0.0.0 to 1.1.4, from 1.2.0 to 1.2.5, from 1.3.0 to 1.3.1. |
| CVE-2026-6371 | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Limatek System Inc. LimRAD NAC allows Stored XSS. This issue affects LimRAD NAC: through 08072026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-13238 | Incorrect Authorization vulnerability in Drupal Commerce Realex / Global Payments allows Forceful Browsing. This issue affects Commerce Realex / Global Payments versions: from 0.0.0 to 3.0.2. |
| CVE-2026-53624 | Fiber is an Express inspired web framework written in Go. Prior to 3.4.0, the helmet middleware in middleware/helmet/helmet.go never sets the Strict-Transport-Security response header even when HSTSMaxAge is configured because it checks c.Protocol() for https instead of c.Scheme(). This issue is fixed in version 3.4.0. |
| CVE-2026-12478 | The fix for CVE-2026-0716 (commit 6ff7ef0, libsoup 3.6.6) placed the integer overflow guard inside the if (masked) block, leaving unmasked server-to-client frames unprotected. A malicious WebSocket server can send a crafted unmasked frame with a payload length near UINT64_MAX to trigger an OOB read in a libsoup-based client when max_incoming_payload_size is set to 0. |
| CVE-2026-54800 | A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.20), SICORE Base system (All versions < V26.20.0). The affected application ships with a default configuration that disables all OPC UA security mechanisms. This could allow an attacker to gain unauthorized access and control over critical system functions. |
| CVE-2026-56666 | ZITADEL is an open source identity management platform. Prior to 4.15.3, ZITADEL's external identity provider handler checks that the local user's email is verified but does not verify that the external IdP confirmed ownership of the same email before auto-linking by email, allowing a permissive provider account with a victim email address to be linked to the victim's local account. This issue is fixed in version 4.15.3. |
| CVE-2026-59897 | Hono is a Web application framework that provides support for any JavaScript runtime. From 4.3.3 before 4.12.27, the AWS API Gateway v1 adapter can drop a distinct repeated request header value because it de-duplicates values using a substring comparison instead of an exact match, so middleware or application logic that depends on the complete X-Forwarded-For chain, rate limiting, audit logging, or proxy-chain validation can receive incomplete data. This issue is fixed in version 4.12.27. |
| CVE-2026-58657 | Grav before 2.0.0 (affected through 2.0.0-rc.9 and the 2.0 branch) contains a stored CSS injection vulnerability in the Markdown image resize() media action. Prior media hardening rejects direct ?style= payloads and unsafe attribute() fallbacks, but the resize() action in Excerpts::processMediaActions() writes caller-controlled values directly into the image's styleAttributes. A lower-privileged content editor who can edit page Markdown can store a crafted image URL with semicolon-delimited CSS declarations in the resize parameters, which are rendered into the final <img style=...> attribute when a higher-privileged reviewer/admin views the page or preview. This does not require JavaScript execution but enables UI redress/overlay and content-manipulation attacks (e.g., a full-viewport fixed overlay). Fixed in 2.0.0. |

| | |
|---|---|
| CVE-2026-55481 | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, default.blade.php renders header_color and related branding color settings inside a CSS style block with HTML escaping that is insufficient for the CSS context, allowing a superadmin to inject arbitrary CSS that affects authenticated users on subsequent page loads when Content Security Policy is disabled. This issue is fixed in version 8.6.2. |
| CVE-2026-56763 | Hono before 4.12.7 allows __proto__ key in parseBody with dot option enabled, permitting specially crafted form field names to create objects with __proto__ properties. When parsed results are merged into regular JavaScript objects using unsafe merge patterns, attackers can exploit this to achieve prototype pollution and modify object behavior. |
| CVE-2026-55890 | Grav is a file-based Web platform. Prior to 2.0.0-rc.9, Grav's incomplete fix for stored XSS through the Markdown media attribute action (CVE-2026-42841) leaves the sibling MediaObjectTrait::style method reachable through the same Markdown excerpt-action pipeline, allowing an editor to save Markdown image style parameters that are written into the rendered img style attribute without sanitization. This issue is fixed in version 2.0.0-rc.9. |
| CVE-2026-59998 | sshd in OpenSSH before 10.4 has an undocumented security-relevant behavior: GSSAPIStrictAcceptorCheck has no value if the server is in Windows Active Directory. |
| CVE-2026-57213 | RabbitMQ is a messaging and streaming broker. Prior to 3.13.14, 4.0.19, 4.1.10, and 4.2.5, the rabbitmq_federation_management plugin renders the consumer_tag field on the Federation Status page without HTML escaping, allowing a user who can configure a federation upstream or policy to execute JavaScript in the browser of a user viewing that page. This issue is fixed in versions 3.13.14, 4.0.19, 4.1.10, and 4.2.5. |
| CVE-2026-15518 | A vulnerability has been found in AREA 17 Twill CMS up to 3.6.0. The impacted element is the function FileLibraryController::storeFile of the file src/Http/Controllers/Admin/FileLibraryController.php of the component Media Library Insert Page. Such manipulation of the argument qqfilename leads to unrestricted upload. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-50312 | Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally. |
| CVE-2026-44760 | Due to a Cross-Site Scripting (XSS) vulnerability, applications based on Business Server Pages framework in SAP NetWeaver Application Server ABAP reflects unsanitized input into the HTTP response which allows an attacker to inject and execute arbitrary JavaScript code under certain conditions. Successful exploitation could allow the attacker to steal session information, perform authenticated actions on behalf of the victim user etc. This vulnerability has low impact on confidentiality and integrity of the data and no impact on application 's availability. |
| CVE-2026-59947 | Composer is a dependency Manager for the PHP language. Prior to 2.2.29 and 2.10.2, when Composer is run with -vvv debug verbosity, it could print a credential embedded in the username slot of a repository or package URL, such as a GitHub Personal Access Token in https://TOKEN@host/, to debug output because AuthHelper, Url::sanitize, and ProcessExecutor did not sanitize username-only URL credentials. This issue is fixed in versions 2.2.29 and 2.10.2. |
| CVE-2026-14361 | The consul-template library before version 0.42.1 is vulnerable to a path redirection issue in the writeToFile template helper that may allow template output to be written outside the intended directory or to overwrite an existing file. This vulnerability (CVE-2026-14361) is fixed in consul-template 0.42.1. |
| CVE-2026-50310 | Integer overflow or wraparound in Windows Devices Human Interface allows an authorized attacker to disclose information locally. |
| CVE-2026-15700 | A security flaw has been discovered in DedeCMS 5.7.118. Affected by this vulnerability is the function ExtractFile of the file include/zip.class.php of the component Album Publishing Feature. The manipulation of the argument filename results in path traversal. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. |
| CVE-2026-15173 | pcapng file parser crash in Wireshark 4.6.0 to 4.6.6 allows denial of service |
| CVE-2026-15539 | A security vulnerability has been detected in SourceCodester Online Book Store System 1.0. Impacted is an unknown function of the file /admin/index.php?page=books of the component Book Image Upload Feature. Such manipulation leads to unrestricted upload. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. |
| CVE-2026-57031 | An Improper Check for Unusual or Exceptional Conditions vulnerability in the packet forwarding engine (PFE) of Juniper Networks Junos OS on MX Series allows adjacent subscribers to bypass configured firewall filters. On MX Series devices with MPC10/11, LC4800/9600, and MX304 with subscribers configured on static interfaces, ingress firewall filters are not enforced, so that neither protocol level nor upstream bandwidth limitation are in effect. This issue affects Junos OS on MX with MPC10/11, LC4800/9600/4802, and MX304: * 23.2 versions from 23.2R2-S1 before 23.2R2-S7, * 23.4 versions from 23.4R2 before 23.4R2-S7, * 24.2 versions before 24.2R2-S3, * 24.4 versions before 24.4R2-S2, * 25.2 versions before 25.2R2. |
| CVE-2026-59883 | Guzzle is an extensible PHP HTTP client. Prior to 7.12.3, CookieJar did not restrict cookies scoped to IP-address or bare-numeric Domain values to the exact host that set them, because SetCookie::matchesDomain() applied ordinary suffix matching to domains such as 192.168.0.1, [::1], or 1, allowing cross-host cookie disclosure, cookie injection, or session fixation. This issue is fixed in version 7.12.3. |
| CVE-2026-54344 | ToolJet is an open-source low-code platform for building internal tools. Prior to 3.20.180, ToolJet's render preview deployment workflow interpolates github.event.comment.body directly into a bash conditional in a run step, allowing any GitHub user who can comment on an open pull request with a deploy command to execute shell commands on the CI runner and exfiltrate deployment secrets. This issue is reported as fixed in version 3.20.180. |
| CVE-2026-54432 | Roundcube Webmail before 1.6.17 and 1.7.x before 1.7.2 allows Stored Cross-Site Scripting (XSS). The issue occurs because the attachment MIME type is not properly escaped on the attachment-validation warning page. |
| CVE-2026-12002 | The Smash Balloon Social Photo Feed – Easy Social Feeds Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.11.1. This is due to missing or incorrect nonce validation on the maybe_connection_data function. This makes it possible for unauthenticated attackers to overwrite the site's Instagram and Facebook oEmbed access tokens via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. |
| CVE-2026-15533 | A security flaw has been discovered in DedeCMS 5.7.118. Impacted is an unknown function of the file /plus/search.php of the component Column Management. Performing a manipulation of the argument Column Name results in code injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. |
| CVE-2026-15494 | A flaw has been found in AMTT Hotel Broadband Operation System 1.0. Impacted is an unknown function of the file manager/network/switch_status.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way. |

| | |
|---|---|
| CVE-2026-49167 | Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally. |
| CVE-2026-49794 | Out-of-bounds read in Windows USB Audio Class driver (usbaudio.sys) allows an unauthorized attacker to disclose information with a physical attack. |
| CVE-2025-30008 | HestiaCP before 1.9.5 contains a stored cross-site scripting vulnerability that allows authenticated low-privilege users to inject arbitrary HTML by creating a DNS record with a double-quote followed by a script payload in the value field. The application fails to apply htmlspecialchars() encoding to the DNS record value field rendered into the data-sort-value HTML attribute in list_dns_rec.php, allowing the payload to execute in the browser of any user who views the DNS record list, including administrators. |
| CVE-2026-61456 | The Grav API plugin (getgrav/grav-plugin-api) before 1.0.3 fails to sanitize SVG files uploaded through the POST /api/v1/media endpoint. The HandlesMediaUploads::processUploadedFile() method validates only the file extension and never invokes Security::sanitizeSVG(), so an authenticated attacker with the api.media.write permission can upload an SVG containing arbitrary JavaScript. The file is stored unmodified and served with Content-Type: image/svg+xml; when an administrator opens it in a browser (directly or via <object>/<iframe>), the embedded script executes in their session context, enabling cookie theft and session hijacking. |
| CVE-2026-8650 | Relative path traversal vulnerability in Progress MOVEit Transfer (Admin Settings module). This issue affects MOVEit Transfer: before 2025.0.7, from 2025.1.0 before 2025.1.3. |
| CVE-2026-54776 | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, a CoreWCF service hosted on Unix Domain Sockets with PosixIdentity client credentials can accept connections that skip the application/unixposix stream upgrade before dispatching messages, bypassing framing-layer identity checks in UnixPosixIdentitySecurityUpgradeProvider. This issue is fixed in versions 1.8.1 and 1.9.1. |
| CVE-2026-59831 | GitHub CLI (gh) is GitHub's official command line tool. From 2.10.0 through 2.95.0, connecting to a malicious Codespace with gh codespace jupyter can allow command execution because the command opens a JupyterLab URL supplied by a process inside the Codespace without validating that it is a loopback HTTP or HTTPS address, allowing a crafted vscode:// or vscode-insiders:// URL to be handed to VS Code. This issue is fixed in version 2.96.0. |
| CVE-2026-11898 | The White Label CMS plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.7.12 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. |
| CVE-2026-11591 | The Widgets for Google Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 13.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. |
| CVE-2026-12108 | The Highlighting Code Block plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.2.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. |
| CVE-2026-3367 | The Lockme OAuth2 calendars integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'App ID' setting in all versions up to, and including, 2.11.0. This is due to insufficient input sanitization and output escaping. The register_setting() call on line 197 lacks a sanitize callback, allowing unsanitized data to be stored via update_option(). When the settings page is rendered, the stored value is echoed directly into an HTML input's value attribute without esc_attr() on line 212. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in the settings page that will execute whenever a user accesses the plugin settings page. Multiple fields are affected: App ID (client_id), App Secret (client_secret), Bookings ID prefix (id_prefix), and API domain (api_domain). This vulnerability is particularly impactful in WordPress multisite installations where administrators of individual sites should not be able to execute JavaScript affecting other users. |
| CVE-2026-15295 | The WordPress Infinite Scroll – Ajax Load More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 7.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. |
| CVE-2026-21901 | A NULL Pointer Dereference vulnerability in the management daemon (mgd) of Juniper Networks Junos OS and Junos OS Evolved allows a local, high-privileged attacker setting or deactivating a specific SSH configuration parameter to create a Denial of Service (DoS). A local high-privileged user configuring or deactivating a specific 'system services ssh' configuration parameter can exploit a null pointer dereference in one of the functions used by SSH. The function attempts to dereference a null pointer when accessing certain configuration data, resulting in an mgd process crash and restart. Continued execution of these configuration commands will create a sustained Denial of Service (DoS) condition. This issue affects: Junos OS: * from 22.3 before 22.3R3-S5; * from 22.4 before 22.4R3-S10; * from 23.2 before 23.2R2-S7; * from 23.4 before 23.4R2-S8. This issue does not affect Junos OS before 22.3R1. Junos OS Evolved: * from 22.3R1-EVO before 23.2R2-S7-EVO; * from 23.4 before 23.4R2-S8-EVO. This issue does not affect Junos OS Evolved before 22.3R1-EVO. |
| CVE-2026-15283 | The WPvivid Backup for MainWP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 0.9.33 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. |
| CVE-2026-12041 | The Chatra Live Chat + ChatBot + Cart Saver plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0.12 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. |
| CVE-2026-9738 | The Print, PDF, Email by PrintFriendly plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'content_position_css' parameter in all versions up to, and including, 5.5.10 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. |
| CVE-2026-46388 | osquery is a SQL powered operating system instrumentation, monitoring, and analytics framework. Prior to 5.23.1, an unprivileged attacker can read the contents of an osquery file carve until the carve completes and the temporary files are deleted because in-progress carve directories are not created with private permissions. If the carve targets a directory that the attacker controls, arbitrary file reads are possible, such as sensitive local files. This issue is fixed in version 5.23.1. |
| | The Gutenberg Blocks with AI by Kadence WP – Page Builder Features plugin for WordPress is vulnerable to unauthorized post publication in all versions up to, and |

| | |
|---|---|
| CVE-2026-15286 | including, 3.5.32 due to a misconfigured capability check on the 'get_items_permission_check' function permission callback of the 'process_pattern' REST API endpoint. This makes it possible for authenticated attackers, with Contributor-level access and above, to create and immediately publish posts of any type (including pages), bypassing the standard WordPress review workflow where contributors must submit posts for administrator approval. |
| CVE-2026-62641 | In Roundcube Webmail before 1.6.17 and 1.7.x before 1.7.2, the TNEF decoder was subject to denial of service via a crafted compressed-RTF size. |
| CVE-2026-62642 | In Roundcube Webmail before 1.6.17 and 1.7.x before 1.7.2, an infinite loop was discovered in the TNEF decoder, which may lead to denial of service upon opening an email with a TNEF attachment. |
| CVE-2026-59930 | Mistune is a Python Markdown parser with renderers and plugins. Prior to 3.3.0, the toc plugin and TableOfContents directive generate heading IDs as predictable toc_N values without slugifying the heading text, allowing attacker-controlled id="toc_N" content to collide with generated anchors and redirect same-page navigation, CSS selectors, or JavaScript handlers. This issue is fixed in version 3.3.0. |
| CVE-2026-15329 | A vulnerability was found in zhayujie CowAgent up to 2.1.0. This issue affects the function BrowserTool._do_navigate of the file agent/tools/browser/browser_tool.py of the component Browser Tool. Performing a manipulation results in information disclosure. The attack can be initiated 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. |
| CVE-2026-58654 | The Grav API plugin (getgrav/grav-plugin-api) 1.0.0 contains an unrestricted file upload vulnerability in the avatar upload endpoint (/api/v1/users/user/avatar). The endpoint validates only the client-declared MIME type (getClientMediaType) beginning with 'image/' and does not inspect the actual file content or restrict the resulting extension, allowing an authenticated user to store arbitrary content — including PHP code, SVG with embedded JavaScript, and polyglot payloads — under user/accounts/avatars/ with predictable filenames. Direct HTTP access to the stored files is blocked by .htaccess (returns 403), but the files persist on disk and could lead to remote code execution or stored XSS in the presence of a path traversal flaw or server misconfiguration. Fixed in 1.0.1. |
| CVE-2026-58209 | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.3 and 2.12.12, MQTT retained message delivery and QoS1+ durable replay could deliver messages whose original topics matched a subscriber configured subscribe deny rule because these delivery paths did not consistently recheck the concrete original topic before sending the MQTT PUBLISH to the subscriber. This issue is fixed in versions 2.14.3 and 2.12.12. |
| CVE-2026-7492 | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 9.1 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an unauthenticated user to determine the existence of a private project due to improper authorization controls on cross-project reference pages. |
| CVE-2026-11359 | The Memberships and User Profiles for WooCommerce – ProfileGrid WooCommerce Integration plugin for WordPress is vulnerable to unauthorized plugin installation and activation in versions up to, and including, 3.4. This is due to a missing capability check and missing nonce validation on the pg_install_profilegrid() AJAX handler registered via wp_ajax_pg_install_profilegrid. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install and activate the ProfileGrid plugin from wordpress. |
| CVE-2026-15131 | Inappropriate implementation in Navigation in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to bypass site isolation via a crafted HTML page. (Chromium security severity: Medium) |
| CVE-2026-15130 | Insufficient policy enforcement in Navigation in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to bypass site isolation via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-15124 | Insufficient policy enforcement in Passwords in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-15108 | Integer overflow in Extensions API in Google Chrome prior to 150.0.7871.115 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted Chrome Extension. (Chromium security severity: High) |
| CVE-2026-12433 | The Hydra Booking – Appointment Scheduling & Booking Calendar plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 1.2.1 via the /wp-json/hydra-booking/v1/booking/details/{id} REST endpoint. This is due to the getBookingDetails() callback only enforcing the tfhb_manage_options capability via tfhb_manage_options_permission(), without verifying that the requested booking belongs to the currently authenticated host (the lookup in getBookingDetailsData() filters solely on the booking id supplied in the URL). This makes it possible for authenticated attackers, with Hydra Host-level access and above (a role created by the plugin which grants tfhb_manage_options), to view sensitive booking records belonging to other hosts, including attendee names, emails, phone numbers, addresses, meeting details, payment method and status, transaction history, and internal notes by iterating booking IDs. |
| CVE-2026-15715 | A vulnerability was identified in SourceCodester Class and Exam Timetabling System 1.0. Affected by this vulnerability is an unknown functionality of the file /exam.php. Such manipulation of the argument day leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be used. |
| CVE-2026-4298 | The DSGVO All in one for WP plugin for WordPress is vulnerable to Missing Authorization in all versions up to and including 4.9. This is due to the dsgvo_reset_policy_service_func() function lacking both capability checks and nonce verification while processing user-supplied parameters to reset plugin options. This makes it possible for authenticated attackers, with Subscriber-level access and above, to reset all customized privacy policy content including cookie notices, Google Analytics policies, Facebook policies, and YouTube policies to their default values. |
| CVE-2026-8472 | GitLab has remediated an issue in GitLab EE affecting all versions from 18.9 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an authenticated user with minimal access permissions to read work item metadata from private projects due to missing authorization checks. |
| CVE-2026-9235 | The DHL eCommerce (Benelux) for WooCommerce plugin for WordPress is vulnerable to unauthorized modification and loss of data due to a missing capability check and missing nonce verification on the create_label() and delete_label() functions in versions up to, and including, 2.2.3. These functions are wired to the wp_ajax_dhlpwc_label_create and wp_ajax_dhlpwc_label_delete hooks and act on an attacker-supplied post_id (WooCommerce order ID). This makes it possible for authenticated attackers, with Subscriber-level access and above, to create or delete DHL shipping labels associated with any WooCommerce order on the site. |
| CVE-2026-9237 | The Employee, Leave and Recruitment Management System – Crew HRM plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.2.2. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete, archive, unarchive, and duplicate arbitrary job listings — along with their associated stages, meta, addresses, and applications — by supplying an arbitrary integer job_id. The nonce verified by Dispatcher::dispatch() is exposed to all authenticated front-end visitors via wp_head script localization, meaning subscribers can trivially obtain it and satisfy the nonce check without possessing any elevated privilege. |
| | The Colissimo Officiel : Méthodes de livraison pour WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the updateShippingMethod() function (registered to the wp_ajax_lpc_order_affect AJAX action) in versions up to, and including, 2.9.0. This is |

| | |
|---|---|
| CVE-2026-9240 | due to the handler performing no current_user_can() capability check and no nonce verification before reading an attacker-supplied order_id and modifying that order's shipping method, pickup-point meta, and shipping address. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create or modify the shipment information (shipping method, pickup relay data, and shipping address) of arbitrary WooCommerce orders, including orders placed by other users. |
| CVE-2026-56298 | Capgo before 12.128.2 fails to strip EXIF metadata from images uploaded via the app information endpoint, exposing sensitive geolocation data. Attackers can upload images containing EXIF metadata to extract geographic location information and other embedded metadata from uploaded files. |
| CVE-2026-58214 | NATS Server is a high-performance server for NATS.io, the cloud and edge native messaging system. Prior to 2.14.3 and 2.12.12, an authenticated MQTT client could subscribe to the internal $MQTT.deliver.pubrel subject family, bypassing configured subscribe permissions and exposing MQTT QoS2 protocol metadata for sessions in the account. This issue is fixed in versions 2.14.3 and 2.12.12. |
| CVE-2026-15187 | A security flaw has been discovered in enquirer up to 2.4.1. Affected is the function Enquirer.set of the component Public Package API. The manipulation of the argument question.name results in improperly controlled modification of object prototype attributes. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report. |
| CVE-2026-55542 | Snipe-IT is an IT asset/license management system. Prior to version 8.6.1, Snipe-IT S3 signature image retrieval lacks authorization before temporary URL. On S3-backed deployments, authenticated users who know a signature filename can obtain a 5-minute signed S3 URL because the S3 branch returns before the `authorize()` call used by the local-file branch. Version 8.6.1 contains a patch. |
| CVE-2026-59217 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.10.0, the file upload path accepted metadata.knowledge_id and auto-linked uploaded files to a target knowledge base without applying the write-access check used by /api/v1/knowledge//file/add, allowing read-only knowledge-base users to add arbitrary files. This issue is fixed in version 0.10.0. |
| CVE-2026-59223 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.10.0, WEB_FETCH_FILTER_LIST matching compared configured host entries against URL strings and non-label-boundary suffixes, allowing path-based blocklist bypasses such as !internal.example.com in a URL path and sibling-domain matches that did not reflect the intended hostname policy. This issue is fixed in version 0.10.0. |
| CVE-2026-59227 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.8.11 before 0.10.0, POST /api/v1/images/edit required only a verified account and did not enforce the global image-edit switch or the per-user image-generation permission, allowing a non-admin user to invoke server-side image editing with administrator-configured provider credentials. This issue is fixed in version 0.10.0. |
| CVE-2026-15202 | A security vulnerability has been detected in YzmCMS up to 7.5. Affected is the function get_url of the file /yzmphp/yzmphp.php of the component Header Handler. The manipulation of the argument HTTP_HOST leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-11992 | The Easy Appointments plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.12.27. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with author-level access and above, to cancel all upcoming appointments site-wide by marking every future appointment stored by the plugin as abandoned. The nonce required to authenticate the cancellation request is printed on the Appointments admin page, which is itself gated only by the edit_posts capability that Authors possess, making the nonce readily accessible to low-privileged users. |
| CVE-2026-15036 | A vulnerability was determined in Harness up to 2.28.2. This vulnerability affects the function getAuthorizedSpaces of the file app/api/controller/gitspace/list_all.go of the component gitspaces Endpoint. Executing a manipulation can lead to authorization bypass. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-55873 | SeaweedFS is a distributed storage system. In versions 4.08 through 4.33, requests signed with SigV4 service s3tables are routed to the S3Tables management API where authorization collapses account-less S3 identities into the shared admin account and fails open, allowing an authenticated low-privileged S3 user to enumerate administrator-owned table bucket names and ARNs. This issue is fixed in version 4.34. |
| CVE-2026-56217 | Capgo before 12.128.2 contains a policy bypass vulnerability in app_versions update enforcement that allows app-scoped API keys to downgrade encrypted bundles to non-encrypted state. Attackers with app-scoped all API keys can directly update the app_versions table via PostgREST to clear session_key and key_id fields, bypassing organization-enforced encrypted-bundle policies and weakening OTA security controls. |
| CVE-2026-33799 | An Out-of-bounds Write vulnerability in the SNMP daemon (snmpd) of Juniper Networks Junos OS and Junos OS Evolved allows an authenticated network-based attacker sending specific valid SNMPv3 queries to trigger a memory leak. Over time, continuous receipt of these queries will result in snmpd process memory exhaustion, resulting in a process crash and restart, impacting the ability to monitor the system via SNMP. Memory usage can be monitored using the following command: user@device> show system processes extensive \| match snmpd This issue affects: Junos OS: * all versions before 21.2R3-S8; * from 21.4 before 21.4R3-S7; * from 22.1 before 22.1R3-S6; * from 22.2 before 22.2R3-S4; * from 22.3 before 22.3R3-S3; * from 22.4 before 22.4R3-S2; * from 23.2 before 23.2R2; * from 23.4 before 23.4R2. Junos OS Evolved: * all versions before 21.2R3-S8-EVO; * from 21.4 before 21.4R3-S7-EVO; * all versions of 22.1-EVO, * from 22.2 before 22.2R3-S4-EVO; * from 22.3 before 22.3R3-S3-EVO; * all versions of 22.4-EVO, * from 23.2 before 23.2R2-EVO; * from 23.4 before 23.4R2-EVO. |
| CVE-2026-9731 | The Wp Js Detect plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.9. This is due to missing or incorrect nonce validation on the plugin_settings function. This makes it possible for unauthenticated attackers to update the plugin's notification text and CSS settings (wp_non_js_notification_text and wp_non_js_notification_css), injecting arbitrary content that is echoed unescaped on the frontend via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. |
| CVE-2026-15034 | A vulnerability has been found in flask-dashboard Flask-MonitoringDashboard up to 5.0.2. Affected by this issue is some unknown functionality. Such manipulation leads to cross-site request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-59840 | A buffer over-read vulnerability in Fortinet FortiOS 7.6.0 through 7.6.2, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2 all versions, FortiProxy 7.6.0 through 7.6.5, FortiProxy 7.4.0 through 7.4.13, FortiProxy 7.2 all versions may allow attacker to information disclosure via <insert attack vector here> |
| CVE-2026-15595 | A vulnerability was determined in SourceCodester Class and Exam Timetabling System 1.0. The affected element is an unknown function of the file /forsubject.php. This manipulation of the argument subject causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. |
| CVE-2026-44770 | SAP Create Single Payment does not perform necessary authorization checks for an authenticated user, a restricted user could access specific entity set keys resulting in disclosure of information. This has low impact on confidentiality, with no impact on integrity and availability of the application. |
| CVE-2026-6541 | Mattermost versions 11.7.x <= 11.7.1, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to restrict metric configuration changes to the playbook being saved, which allows an authenticated user with team access to alter another user’s playbook metric settings via a crafted import or update request with a foreign metric ID. Mattermost Advisory ID: MMSA-2026-00653 |

| | |
|---|---|
| CVE-2026-9341 | The Academy LMS – WordPress LMS Plugin for Complete eLearning Solution plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.8.0 via the 'save_lesson_note', 'get_lesson_note', and 'complete_lesson_video' AJAX handlers due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read, overwrite, or delete the private lesson notes of any other user (including administrators), and to falsify lesson-completion progress for arbitrary users. |
| CVE-2026-15718 | We are aware that exploit code for this is public however we are not aware of any attacks in the wild abusing this flaw. This vulnerability was fixed in Firefox 152.0.6. |
| CVE-2026-62393 | Improper Handling of Insufficient Permissions or Privileges vulnerability in Apache Kylin. Improper authorization in job information retrieval, where an attacker may get access to unauthorized jobs in other projects. This issue affects Apache Kylin: from 4 through 5.0.3. Users are recommended to upgrade to version 5.0.4, which fixes the issue. |
| CVE-2026-10628 | The Points and Rewards for WooCommerce plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.10.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to convert and drain any user's reward points into wallet balance, exfiltrate all users' emails and point balances to an attacker-controlled Klaviyo account, overwrite the site's Klaviyo public API key, block or unblock arbitrary users from the points system, and modify campaign banner and heading settings. The nonce used for authentication of these requests (wps-wpr-verify-nonce) is injected into every public-facing page via wp_localize_script(), and the wps_wpr_generate_custom_wallet handler is additionally registered on the wp_ajax_nopriv_ hook, meaning unauthenticated visitors can also obtain a valid nonce and exploit that specific action. |
| CVE-2026-15492 | A security vulnerability has been detected in igweze wizgrade up to b1d55f22b90cd7e7a6e5002f006d7c649e8086d6. This vulnerability affects unknown code of the file dashboard/studentConductManager.php. Such manipulation leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15474 | A security flaw has been discovered in Eleveo Call Recording Software 9.7.0. Impacted is an unknown function of the file /callrec/audio.jsp of the component Call Recording Handler. The manipulation of the argument callId results in improper authorization. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15472 | A vulnerability was determined in Eleveo Call Recording Software 9.7.0. This vulnerability affects unknown code of the file /callrec/composeEmailAction.do. Executing a manipulation can lead to improper authorization. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-57797 | Missing Authorization vulnerability in ThemeMove EduMall edumall allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects EduMall: from n/a through <= 4.5.1. |
| CVE-2026-7544 | The Mux Video Uploader plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.1.4 via the muxvideo_enqueue_settings_script. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract sensitive data including Mux API credentials. |
| CVE-2026-15471 | A vulnerability was found in Eleveo Call Recording Software 9.7.0. This affects an unknown part of the file /callrec/pci_dss_status.jsp. Performing a manipulation results in improper authorization. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15470 | A vulnerability has been found in Eleveo Call Recording Software 9.7.0. Affected by this issue is some unknown functionality of the file /callrec/group.jsp. Such manipulation leads to improper authorization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-15607 | A vulnerability was detected in tanstack db up to 0.6.8. Affected by this vulnerability is the function select of the file src/query/compiler/select.ts of the component Alias Path Handler. The manipulation results in improperly controlled modification of object prototype attributes. The attack may be launched remotely. The exploit is now public and may be used. The patch is identified as ac09b1177a100eafa85cba3cd09dd1f53f933ded. A patch should be applied to remediate this issue. |
| CVE-2026-58661 | n8n before 2.28.0 (and before 1.123.58 on the 1.x branch) contains a disk space exhaustion vulnerability in the data-table file upload endpoint. The per-request quota check does not account for files already written to the shared temporary directory, allowing an authenticated user to repeatedly upload files that accumulate on disk until the periodic cleanup runs, potentially exhausting available disk space on the host. |
| CVE-2026-8678 | The MyParcel plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.25.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to view and modify shipment options — including carrier, delivery type, package type, number of labels, weight, signature requirement, and insurance — on any arbitrary order. |
| CVE-2026-13116 | The PDF Invoices & Packing Slips for WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.14.0 via the generate_document_shortcode due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with contributor-level access and above, to mint publicly accessible, session-free download links for arbitrary third-party orders, exposing customer names, billing and shipping addresses, email addresses, phone numbers, order and invoice numbers, line items, totals, payment details, and customer notes contained in those orders' invoices and packing slips. Exploitation requires the plugin's Document link access type setting to be configured to 'full'; with the default 'logged_in' value, generated URLs are signed with a per-session nonce rather than the order_key, making the shortcode path unexploitable for unauthorized access to third-party orders. |
| CVE-2026-1832 | The ThriveDesk – Live Chat, AI Chatbot, Helpdesk & Knowledge Base plugin for WordPress is vulnerable to unauthorized cache deletion due to a missing capability check on the 'thrivedesk_clear_cache' AJAX action in all versions up to, and including, 2.1.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to clear the plugin's cache. |
| CVE-2026-3552 | The SurfLink - Ultimate Link Manager plugin for WordPress is vulnerable to unauthorized data modification due to a missing capability check on the ajax_import_410() function in all versions up to 2.6.0. This is due to a missing capability check (current_user_can()) and missing nonce verification (check_ajax_referer()) in the ajax_import_410() function, while all other AJAX handlers in the same class (ajax_add_single_410, ajax_save_editted_410, ajax_delete_410, ajax_bulk_410_delete, ajax_empty_410, ajax_export_410) properly implement both authorization and nonce checks. This makes it possible for authenticated attackers, with Subscriber-level access and above, to import arbitrary URLs into the 410 Gone database table via the surfl_import_410 AJAX action. Injected URLs will cause the site to return HTTP 410 Gone responses to all visitors accessing those paths, potentially causing denial of service for legitimate pages and SEO damage through search engine delisting. |
| CVE-2026-55472 | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, when Full Multiple Companies Support and scope_locations_fmcs are enabled, the API location creation endpoint detects an invalid parent-child company mismatch but does not return immediately, allowing creation of a child location under a parent location from a different company. This issue is fixed in version 8.6.2. |
| CVE- | Snipe-IT is an IT asset/license management system. Prior to 8.6.0, POST /account/request/{itemType}/{itemId}/{cancel_by_admin?}/{requestingUser?} accepts |

| | |
|---|---|
| 2026-55476 | cancel_by_admin as a URL path segment without sufficient authorization, allowing an authenticated user to supply a victim user ID and silently cancel that user's pending asset requests. This issue is fixed in version 8.6.0. |
| CVE-2026-7559 | The Affilia – Affiliate Program & Referral Tracking for WordPress plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 3.3.3. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to approve or reject affiliate referrals, credit commissions to affiliate wallets, delete referral records, and modify custom banner plugin options, enabling financial fraud. The nonce required to pass the only authentication check is embedded in every frontend page load via rtwalwm_global_params.rtwalwm_nonce, making it trivially accessible to any authenticated user regardless of role. |
| CVE-2026-9857 | The Invoice123 plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.7.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to overwrite the plugin's API key stored in wp_options, modify invoice plugin settings, and alter WooCommerce tax rate data in the wp_woocommerce_tax_rates table. |
| CVE-2025-43892 | A buffer over-read vulnerability in Fortinet FortiOS 7.6.0 through 7.6.2, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2 all versions may allow an authenticated remote attacker to return a portion of device memory in the redirect response via submitting a specially crafted request. |
| CVE-2026-62198 | OpenClaw versions 2026.5.28 before 2026.6.6 contain an authorization bypass vulnerability in native web search that allows lower-trust callers to perform actions requiring stronger policy checks. Attackers can exploit misconfigured input paths to bypass intended authorization controls and execute restricted operations. |
| CVE-2026-7620 | The Notification for Telegram plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.5.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to create, modify, or reschedule the nftb_cron_hook WordPress cron event, enabling unauthorized manipulation of the plugin's background task scheduling logic. |
| CVE-2026-56240 | Capgo before 12.128.12 contains a billing authorization bypass vulnerability in the plan_valid calculation that allows organizations with exhausted or expired usage credit grants to bypass billing gates. Attackers can exploit the divergence between the plugin hot-path plan_valid expression and the authoritative billing gate to gain continued access to /updates, /stats, /channel_self, and attachment upload endpoints after credit depletion. |
| CVE-2026-10041 | The WCFM – Frontend Manager for WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 6.7.27 via the wcfm_product_archive due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to archive arbitrary vendors' products, toggle the featured status on arbitrary listings, mark arbitrary WooCommerce orders as completed, and permanently delete arbitrary enquiries and bulk messages belonging to other vendors. |
| CVE-2026-12738 | The WP Easy Pay – Payment and Donation form Builder for Square plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.5.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to set the status of arbitrary posts and pages to 'draft', effectively unpublishing arbitrary site content. |
| CVE-2026-9824 | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to check the manage_shared_channels permission in the /share-channel autocomplete handler, which allows an authenticated user without that permission to enumerate configured remote cluster connection metadata via slash command autocomplete.. Mattermost Advisory ID: MMSA-2026-00676 |
| CVE-2026-44771 | SAP S/4HANA Draft operation does not perform necessary authorization checks for an authenticated user, a restricted user could access information within the entity resulting in escalation of privileges. This results in low impact on confidentiality, with no impact on integrity and availability of the application. |
| CVE-2026-15627 | A vulnerability was identified in nextlevelbuilder GoClaw up to 3.13.3-beta.3. This vulnerability affects the function handleNavigate of the file pkg/browser/tool.go. Such manipulation of the argument args.targetUrl leads to information disclosure. The attack may be performed from remote. The exploit is publicly available and might be used. |
| CVE-2026-12400 | The FlowForms – Conversational Form Builder plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.1.1 via the update_form due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with contributor-level access and above, to modify the content, design, and settings of, as well as publish or revert, any form on the site — including forms owned by administrators — by supplying an arbitrary form ID in the REST URL. |
| CVE-2026-12955 | The GDPR Cookie Consent plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check and missing nonce verification on the gdpr_cookie_consent_ajax_save_schedule_scan() function (the wp_ajax_gcc_save_schedule_scan AJAX action) in versions up to, and including, 4.3.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify the plugin's cookie scan schedule configuration stored in the gdpr_scan_schedule_data option, which is an administrative function intended to be limited to users with the manage_options capability. |
| CVE-2026-15026 | The Import and export users and customers plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.4.0 via the email_template_selected. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract the post_title and raw post_content of arbitrary posts regardless of status (draft, private, future, trash, password-protected) or post type (including non-public CPTs such as WooCommerce orders and internal CRM records) by enumerating post IDs. The required codection-security nonce is exposed as inline JavaScript on any wp-admin page when ?post_type=acui_email_template is appended to the URL, which is reachable by any authenticated user including Subscribers. |
| CVE-2026-1946 | The GW AI Website Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the gwaiwebu_gravitywrite_disconnect_handler() function in all versions up to, and including, 1.0.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to disconnect the plugin from GravityWrite via the 'gwaiwebu_gravitywrite_disconnect' AJAX action. |
| CVE-2026-6440 | The GoodMeet – Google Meet Integration for Webinar, Meeting & Video Conference plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to and including 1.1.8. This is due to a missing nonce verification in the reset_credential() function, which handles the wp_ajax_goodmeet_reset_google_meet_credential AJAX action. While the function does verify the user's capability (manage_options), it does not validate a nonce, making it susceptible to CSRF attacks. This makes it possible for unauthenticated attackers to trick a site administrator into clicking a malicious link that will reset (delete) the plugin's stored Google Meet API credentials (goodmeet_google_credentials) and OAuth tokens (goodmeet_google_token), effectively disabling the Google Meet integration on the site. |
| CVE-2026-15377 | A vulnerability was determined in Eleveo Call Recording Software 9.7.0. Affected by this vulnerability is an unknown functionality of the file /callrec/sendlogfile. This manipulation causes improper authorization. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-12385 | The Smart Slider 3 plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.5.1.37 via the 'keyword' parameter. This makes it possible for authenticated attackers, with contributor-level access and above, to extract titles and full content excerpts of private, draft, pending, trashed, and auto-draft posts authored by any user, including Administrators and Editors. The required nonce is emitted on /wp-admin/post-new.php, which is accessible to Contributor-level users via the edit_posts capability, meaning any Contributor can obtain the nonce needed to trigger the injection. |
| CVE-2026- | A vulnerability was identified in SourceCodester Class and Exam Timetabling System 1.0. The impacted element is an unknown function of the file /subject.php. Such manipulation of the argument subject leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be |

| | |
|---|---|
| 15596 | used. |
| CVE-2026-15080 | Cross-Site Request Forgery (CSRF) vulnerability in Drupal Ray Enterprise Translation allows Cross Site Request Forgery. This issue affects Ray Enterprise Translation versions: from 0.0.0 to 4.0.4, from 4.1.0 to 4.1.4, from 11.0.0 to 11.0.4. |
| CVE-2026-15375 | A vulnerability has been found in Eleveo Call Recording Software 9.7.0. This impacts an unknown function of the file /callrec/users_ldap.jsp of the component LDAP User Interface. The manipulation leads to improper authorization. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-55479 | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, the legacy single-seat license checkin flow authorizes the action with the checkout permission instead of the checkin permission, allowing a user who can assign licenses but not unassign them to directly access the old checkin endpoint and reclaim a license seat assigned to another user or asset. This issue is fixed in version 8.6.2. |
| CVE-2026-55664 | Grist is spreadsheet software using Python as its formula language. Prior to 1.7.15, the GET /forms endpoint read table and column metadata without applying the document's access rules and did not check that the requested section was actually a form. A user with only partial read access, including public access on a publicly viewable document, could request the metadata of any widget and reveal table and column structure that access rules would otherwise hide, even in documents that contain no forms. This issue is fixed in version 1.7.15. |
| CVE-2026-10103 | Mattermost versions 11.7.x <= 11.7.2, 11.6.x <= 11.6.4, 10.11.x <= 10.11.19 fail to verify post ownership in the shared channel inbound sync handler, which allows an authenticated remote cluster to modify or delete posts authored by local users or other remotes via crafted sync messages referencing arbitrary post IDs in channels shared with that remote.. Mattermost Advisory ID: MMSA-2026-00689 |
| CVE-2026-61502 | Rejetto HFS 3.0.0 through 3.2.0 accepts state-changing API requests via the GET method and exempts GET requests from its anti-CSRF header check. A remote attacker can perform administrative actions including account creation and configuration changes leading to code execution - by causing a logged-in administrator's browser to navigate to a crafted URL, or without any credentials against default installations when the attack originates from the server's own machine. |
| CVE-2026-55462 | Snipe-IT is an IT asset/license management system. Prior to 8.6.2, UsersController::show() and printInventory() authorize only user viewing before loading and rendering assigned license, accessory, and consumable relationships, allowing an authenticated user with only users.view to see inventory and cost/order metadata from modules that direct permissions would otherwise deny. This issue is fixed in version 8.6.2. |
| CVE-2026-13699 | In Eclipse KUKSA Databroker version 0.6.1, the kuksa.val.v2.VAL/PublishValue gRPC handler fails to validate the existence of the optional data_point field in PublishValueRequest. When a request contains a valid signal_id but omits data_point, the server directly calls unwrap() on request.data_point, triggering a panic in the Tokio worker thread. This issue can be triggered by any client holding a valid JWT token. Unauthenticated or invalid-token requests are rejected and do not reach the vulnerable path. The panic causes the individual gRPC call to be cancelled but does not terminate the Databroker process, which remains available for subsequent requests. |
| CVE-2026-12273 | The Tutor LMS WordPress plugin before 3.9.13 does not perform any authorization or post-target validation before creating a comment in one of its handlers, and stores the comment pre-approved, allowing authenticated users with subscriber-level access and above to post auto-approved comments containing arbitrary HTML and links on any content across the site, bypassing the comment moderation queue. |
| CVE-2026-59154 | Wekan is open source kanban built with Meteor. Prior to 9.64, Wekan has a cross-board authorization bypass in the direct Meteor collection allow rules for Checklists and ChecklistItems because updates are authorized only against the current source doc.cardId and do not inspect the destination cardId or boardId in the update modifier, allowing a low-privileged authenticated user with write access to one board and knowledge of a target private card id to create checklist data on an accessible card and move it into a private board where they are not a member. This issue is fixed in version 9.64. |
| CVE-2026-12103 | The Wallet for WooCommerce plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.6.4. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to enumerate the login name, email address, and user ID of all WordPress accounts — including administrators — by submitting arbitrary search terms to the AJAX handler. The required 'search-user' nonce is localized into the wallet_param object on the standard WooCommerce My Account page, which is accessible to any authenticated user, making it trivially obtainable by a Subscriber. |
| CVE-2026-12397 | The WP Job Portal WordPress plugin before 2.5.5 does not verify ownership when returning an employer's contact email for a given job, allowing authenticated users with a subscriber-level (self-registerable) account to read other employers' private account email addresses by enumerating job identifiers. |
| CVE-2026-15540 | A vulnerability was detected in SourceCodester Online Book Store System 1.0. The affected element is an unknown function of the file /admin/index.php of the component Administrative Interface. Performing a manipulation of the argument page results in improper control of filename for include/require statement in php program. It is possible to initiate the attack remotely. The exploit is now public and may be used. |
| CVE-2026-59995 | sftp in OpenSSH before 10.4 does not properly constrain the location of downloaded files when "sftp server:/path ." is used with an attacker-controlled server. |
| CVE-2026-59996 | scp in OpenSSH before 10.4 may place a file in the parent directory of an intended directory when the copy occurs between two remote destinations. |
| CVE-2026-59997 | internal-sftp in sshd in OpenSSH before 10.4 recognizes only the first 9 command-line arguments, which can be important if a later command-line argument would have helped to ensure the intended security properties of an SFTP connection. |
| CVE-2026-15083 | Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal ECA: Event - Condition - Action allows Object Injection. This issue affects ECA: Event - Condition - Action versions: from 0.0.0 to 2.1.20, from 3.0.0 to 3.0.12, from 3.1.0 to 3.1.4. |
| CVE-2026-14896 | HashiCorp Nomad and Nomad Enterprise are vulnerable to a cross-namespace authorization bypass in the dynamic host volumes feature that may allow an operator holding the host volume delete permission in one namespace to delete a sticky volume claim belonging to a job in another namespace. This vulnerability, CVE-2026-14896, is fixed in Nomad Community Edition 2.0.4 and Nomad Enterprise 2.0.4, 1.11.8, and 1.10.14. |
| CVE-2026-55669 | ZITADEL is an open source identity management platform. Prior to 3.4.12 and 4.15.2, ZITADEL's external JWT Identity Provider validates a token's signature and issuer (iss) but not the audience (aud) claim, allowing a validly signed token from a trusted issuer for another relying party to be accepted by ZITADEL. This issue is fixed in versions 3.4.12 and 4.15.2. |
| CVE-2026-56664 | ZITADEL is an open source identity management platform. Prior to 3.4.12 and 4.15.2, ZITADEL's external JWT Identity Provider validation in internal/idp/providers/jwt/session.go skips the maximum token age freshness check when an incoming token omits the iat claim, allowing arbitrarily old tokens from a trusted issuer to pass authentication. This issue is fixed in versions 3.4.12 and 4.15.2. |

| | |
|---|---|
| CVE-2026-50302 | Improper certificate validation in Windows Cryptographic Services allows an unauthorized attacker to bypass a security feature over a network. |
| CVE-2026-59882 | guzzlehttp/psr7 is a PSR-7 HTTP message library implementation in PHP. Prior to 2.12.3, Uri::assertValidHost() does not reject URI host components containing authority delimiters, embedded ports, or malformed IPv6 brackets, allowing Uri::getHost() to disagree with the URI authority used for security or routing decisions. This issue is fixed in version 2.12.3. |
| CVE-2026-13236 | Missing Authorization vulnerability in Drupal AI Agents allows Forceful Browsing. This issue affects AI Agents versions: from 0.0.0 to 1.1.4, from 1.2.0 to 1.2.5, from 1.3.0 to 1.3.1. |
| CVE-2026-56665 | ZITADEL is an open source identity management platform. Prior to 3.4.12 and 4.15.2, ZITADEL is an open source identity management platform. From 3.0.0-rc.1 through 3.4.11 and from 4.0.0-rc.1 through 4.15.1, ZITADEL's external JWT Identity Provider validation in internal/idp/providers/jwt/session.go skips expiration handling when an incoming token omits the exp claim, allowing a token from a trusted issuer to be treated as valid without an automatic expiration window. This issue is fixed in versions 3.4.12 and 4.15.2. |
| CVE-2026-44768 | SAP CRM WebClient UI allows an attacker to inject and execute malicious scripts in the context of the application due to the absence of a Content Security Policy (CSP) configuration for certain restrictive directives. This vulnerability has a low impact on the integrity of the application. Confidentiality and availability are not impacted. |
| CVE-2026-56354 | n8n before 1.123.24, 2.10.4, and 2.12.0 (across its 1.x and 2.x branches) contains cross-site scripting and open redirect vulnerabilities in the Form Node due to unsanitized HTML description fields and overly permissive iframe sandbox policies. Authenticated users with workflow creation permissions can inject malicious scripts or redirect parameters to perform stored XSS attacks or phishing redirects against end users. |
| CVE-2026-14902 | An open redirect in Ivanti Xtraction before version 2026.2.1 allows a remote unauthenticated attacker to redirect users to arbitrary external URLs. |
| CVE-2026-56360 | n8n before versions 1.123.18 and 2.6.2 fails to verify HMAC-SHA256 signatures on Zendesk webhooks in the ZendeskTrigger node. Attackers who know the webhook URL can send unsigned POST requests to trigger workflows with arbitrary malicious data. |
| CVE-2026-15028 | A flaw was found in libarchive. This vulnerability allows a remote attacker to trigger a heap overflow by providing a specially crafted tar archive. The issue occurs during the parsing of a PAX extended header containing a malformed SUN.holesdata sparse-file attribute. Successful exploitation could lead to a denial of service, making the system unavailable, or potentially allow for arbitrary code execution, giving the attacker control over the affected system. |
| CVE-2026-59269 | A user authenticating to Kubernetes clusters via the Pinniped Supervisor could potentially gain elevated permissions in the clusters, only if all the following conditions were true: the Pinniped Supervisor server is running with an ActiveDirectoryIdentityProvider resource configured; the ActiveDirectoryIdentityProvider.spec.groupSearch.attributes.groupName is empty; the attacker gains the ability to edit some part of the distinguished name (DN) of group entries in the Active Directory (AD) server's database for groups to which they belong; the configured group search parameters cause the edited group to be included in the group search results for the user; and the attacker knows the password for an AD user who belongs to the edited AD group. Affected versions: Pinniped (go.pinniped.dev) v0.11.0 through v0.46.0 inclusive; fixed in v0.47.0. |
| CVE-2026-15326 | A vulnerability was identified in halo-dev halo up to 2.24.2. This affects the function ThemeUtils.unzipThemeTo of the file ThemeUtils.java of the component Theme Installation. Such manipulation of the argument metadata.name leads to path traversal. The attack may be launched remotely. The exploit is publicly available and might be used. The project closed the issue as "duplicate" but did not reference any other issue, report, or CVE. |
| CVE-2026-9820 | Mattermost versions 11.7.x <= 11.7.2, 10.11.x <= 10.11.19 fail to sanitize team objects returned by the scheme teams endpoint, which allows a user with the User Manager role to obtain invite links for private teams and use them to join or share access to those teams via the scheme teams API endpoint.. Mattermost Advisory ID: MMSA-2026-00671 |
| CVE-2026-56281 | Capgo before 12.128.2 contains a sql injection vulnerability in the POST /private/admin_stats endpoint where the limit parameter is destructured from unvalidated request body and interpolated directly into Cloudflare Analytics Engine SQL queries via template literals. An attacker with platform admin credentials can inject SQL fragments to enumerate dataset schemas, extract analytics data, or cause denial-of-service against the analytics backend. |
| CVE-2026-15594 | A vulnerability was found in waooAI waoowaoo up to 0.4.1. Impacted is the function stablePublicIdFromStorageKey in the library src/lib/media/hash.ts of the component Media Handler. The manipulation of the argument storageKey results in improper authorization. The attack may be performed from remote. The attack requires a high level of complexity. The exploitability is considered difficult. The 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. |
| CVE-2026-8651 | Limited authentication bypass by spoofing vulnerability in Progress MOVEit Transfer (HTTPS module). This issue affects MOVEit Transfer: before 2025.0.7, from 2025.1.0 before 2025.1.3. |
| CVE-2026-60000 | sshd in OpenSSH before 10.4 allows remote attackers to cause a denial of service (resource consumption from excessive authentication attempts) because MaxAuthTries was mishandled for GSSAPIAuthentication. |
| CVE-2026-12590 | Impact: In body-parser versions prior to 1.20.6 (1.x line) and 2.3.0 (2.x line), when the parser is configured with an invalid limit option value such as an unparseable string or NaN, bytes.parse returns null and the request body size check is silently skipped. Applications that rely on limit as their primary safeguard against oversized request bodies will accept arbitrarily large payloads, leading to excessive memory and CPU usage and denial of service. Patches: This issue is fixed in body-parser 1.20.6 and 2.3.0. After the fix, invalid limit values throw a clear error at parser construction time instead of silently disabling enforcement, while null and undefined continue to fall back to the default limit of 100kb. Workarounds: Validate the limit value before passing it to body-parser. For example, parse the value at startup and reject any configuration where the result is null or a non-finite number. |
| CVE-2026-15041 | A flaw was found in 389 Directory Server. The PBKDF2-SHA256 password verification function uses standard memcmp() for comparing password hashes instead of a constant-time comparison function. A remote attacker could potentially use timing measurements of LDAP bind attempts to infer partial hash information, though practical exploitation is extremely difficult due to PBKDF2 computational overhead. |
| CVE-2026-61861 | ImageMagick before 7.1.2-26 contains a use-after-free vulnerability in the FormatMagickCaption method when memory allocation fails. Attackers can trigger memory allocation failures to cause a dangling pointer to reference freed memory, potentially enabling denial of service or code execution. |
| CVE-2026-54780 | CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. Prior to 1.8.1 and 1.9.1, the CoreWCF WS-Security 1.0 receive pipeline validates ds:SignedInfo SignatureMethod against the configured SecurityAlgorithmSuite but does not validate each ds:Reference DigestMethod, allowing a sender to use a rejected digest algorithm such as SHA-1 while the message is still accepted. This issue is fixed in versions 1.8.1 and 1.9.1. |

| | |
|---|---|
| CVE-2026-56373 | ImageMagick before 7.1.2-15 contains a use-after-free vulnerability in the PDB decoder that uses a stale pointer when memory allocation fails. Attackers can trigger this vulnerability by processing malicious PDB files to cause crashes or write a single zero byte to freed memory. |
| CVE-2026-44753 | SAP HANA Database (user self service tools) allows an unauthenticated user to send specially crafted requests that produce distinguishable responses, enabling enumeration of valid user accounts and email addresses. Successful exploitation could allow the attacker to enumerate valid user accounts, resulting in low impact on confidentiality, with no impact on integrity and availability of the application. |
| CVE-2026-61857 | ImageMagick before 7.1.2-26 contains a heap use-after-free vulnerability caused by missing null check when parsing XMP profiles. Attackers can craft malicious image files with specially crafted XMP data to trigger the vulnerability and cause application crashes. |
| CVE-2026-59791 | In JetBrains YouTrack before 2026.2.17012 cSS injection via Mermaid diagram rendering was possible |
| CVE-2025-12506 | GitLab has remediated an issue in GitLab CE/EE affecting all versions from 16.5 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an authenticated user to create a repository where the content displayed in the web interface differed from the content available for download, due to improper handling of Git reference name resolution. |
| CVE-2026-15311 | A vulnerability was identified in NousResearch hermes-agent up to 2026.5.29.2. Affected by this issue is the function MatrixAdapter._markdown_to_html of the file gateway/platforms/matrix.py of the component Matrix Adapter. Such manipulation leads to cross site scripting. The attack can be executed remotely. The exploit is publicly available and might be used. The pull request to fix this issue awaits acceptance. |
| CVE-2026-61492 | In JetBrains YouTrack before 2026.2.17394 stored XSS via article titles in digest emails was possible |
| CVE-2026-59213 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.6.27 before 0.10.0, get_all_models handlers in routers/openai.py and routers/ollama.py passed a lambda to aiocache key instead of key_builder, causing permission-filtered per-user model lists to share a static cache entry and exposing one user’s model list to another caller during the TTL window. This issue is fixed in version 0.10.0. |
| CVE-2026-15678 | A security vulnerability has been detected in code-projects Online Job Portal 1.0. This impacts an unknown function of the file /Admin/DetailJob.php. The manipulation leads to cross site scripting. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. |
| CVE-2026-15505 | A weakness has been identified in vnotex vnote up to 3.20.1. Impacted is an unknown function of the file /src/data/extra/web/js/markdownit.js of the component YAML Frontmatter. This manipulation of the argument p_metaData causes cross site scripting. The attack may be initiated remotely. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2026-8801 | Path equivalence: vulnerability in Progress MOVEit Transfer (File Upload modules). This issue affects MOVEit Transfer: before 2025.0.8, from 2025.1.0 before 2025.1.4. |
| CVE-2026-15493 | A vulnerability was detected in Akpali9 Attendance-Management-System up to 70b91fe38f4195b701a45f0edcd4f42d5f64aeee. This issue affects some unknown processing of the file absent.php. Performing a manipulation of the argument export_date results in cross site scripting. It is possible to initiate the attack remotely. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way. |
| CVE-2025-62675 | An Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting') vulnerability [CWE-113] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.4, FortiOS 7.4 all versions, FortiOS 7.2 all versions, FortiProxy 7.6.0 through 7.6.4, FortiProxy 7.4 all versions, FortiProxy 7.2 all versions may allow an attacker in possession of a valid web filter override token to inject arbitrary headers via tricking a user into clicking on a crafted link. |
| CVE-2026-15274 | A vulnerability was detected in lo48576 fbxcel up to 0.9.0. This affects an unknown part of the file src/pull_parser/v7400/parser.rs of the component Node Header Handler. The manipulation results in denial of service. The attack must be initiated from a local position. The exploit is now public and may be used. The pull request to fix this issue awaits acceptance. |
| CVE-2026-13233 | Server-Side Request Forgery (SSRF) vulnerability in Drupal OpenAI Provider allows Server Side Request Forgery. This issue affects OpenAI Provider versions: from 0.0.0 to 1.1.1, from 1.2.0 to 1.2.2. |
| CVE-2026-52839 | Easy!Appointments is a self hosted appointment scheduler. Versions prior to 1.6.0 correctly filter provider-scoped appointments in the `appointments/search` response, proving that provider isolation is an intended security boundary. However, the direct mutation endpoints `appointments/store` and `appointments/update` only check generic appointment privileges and never verify that the submitted `id_users_provider` belongs to the current session. A normal authenticated provider can inject new appointments into another provider's schedule via `store`, or reassign existing appointments into a foreign provider's calendar via `update`. The `store` path contains an additional write-before-crash bug: the unauthorized row is committed to the database before the controller crashes on a type error, so the attacker receives an error response while the foreign appointment is already persisted. Version 1.6.0 patches the issue. |
| CVE-2026-15528 | A vulnerability was found in lamaalrajih kicad-mcp up to 3.3.1. This issue affects some unknown processing of the file kicad_mcp/utils/path_validator.py. Performing a manipulation of the argument project_path/schematic_path results in protection mechanism failure. Attacking locally is a requirement. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-56362 | ImageMagick before 7.1.2-15 contains a heap-buffer-overflow read vulnerability in GetPixelIndex caused by OpenPixelCache updating image channel metadata before pixel cache memory allocation. Attackers can trigger memory and disk allocation failures to cause a heap-buffer-overflow read affecting any writer calling GetPixelIndex. |
| CVE-2026-61465 | ImageMagick before 7.1.2-26 and 6.9.13-51 is missing a check for the allowed memory allocation limit in matrix-backed operations such as -canny. An attacker can supply a crafted image that causes ImageMagick to allocate more memory than permitted by the configured policy, resulting in a denial of service. |
| CVE-2026-15184 | A vulnerability was found in GNU LibreDWG up to 0.13.4. The impacted element is the function dwg_next_entity of the file src/dwg.c of the component DWG File Handler. Performing a manipulation of the argument next_obj results in null pointer dereference. The attack must be initiated from a local position. The exploit has been made public and could be used. Upgrading to version 0.14 is sufficient to resolve this issue. The patch is named dde45dac3c4d902e4d8fed150a8017b9732019c9. Upgrading the affected component is recommended. Different than CVE-2026-9503. |
| CVE-2026-15526 | A flaw has been found in augmnt augments-mcp-server 7.1.0. This issue affects the function scanProjectDeps of the file src/tools/v4/scan-project-deps.ts of the component scan_project_deps. Executing a manipulation of the argument packageJsonPath can lead to path traversal. The attack can only be executed locally. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet. |

| | |
|---|---|
| CVE-2026-13235 | Missing Authorization vulnerability in Drupal AI (Artificial Intelligence) allows Forceful Browsing. This issue affects AI (Artificial Intelligence) versions: from 0.0.0 to 1.2.17, from 1.3.0 to 1.3.8, from 1.4.0 to 1.4.3. |
| CVE-2026-15524 | A security vulnerability has been detected in alioshr memory-bank-mcp up to 0.2.1/3.1. This affects an unknown part of the file list-project-files-validation-factory.ts. Such manipulation of the argument projectName leads to path traversal. Local access is required to approach this attack. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet. |
| CVE-2026-15194 | A security flaw has been discovered in Open5GS 2.7.7. This affects the function amf_context_final of the file src/amf/context.c of the component AMF. Performing a manipulation results in use after free. The attack is only possible with local access. The exploit has been released to the public and may be used for attacks. |
| CVE-2026-15185 | A vulnerability was determined in GPAC 26.03-DEV. This affects the function vobsub_read_idx of the file /src/media_tools/vobsub.c of the component MP4Box. Executing a manipulation of the argument num_langs can lead to out-of-bounds read. The attack needs to be launched locally. The exploit has been publicly disclosed and may be utilized. This patch is called 532097084729a936bcdf6a27c41003f3bd7dc3ff. It is best practice to apply a patch to resolve this issue. Two different commits were applied to fix this issue. |
| CVE-2026-15276 | A flaw has been found in pdeljanov Symphonia up to 0.6.0. This vulnerability affects unknown code of the component Metadata Handler. This manipulation causes denial of service. The attack needs to be launched locally. The exploit has been published and may be used. The pull request to fix this issue awaits acceptance. |
| CVE-2026-11909 | Missing Authorization vulnerability in Drupal Examples for Developers allows Forceful Browsing. This issue affects Examples for Developers versions: from 0.0.0 to 4.0.6. |
| CVE-2026-56366 | ImageMagick before 7.1.2-18 contains a memory leak vulnerability in the META reader when processing APP1JPEG input paths. Attackers can trigger this memory leak by providing specially crafted APP1JPEG image files, causing denial of service through resource exhaustion. |
| CVE-2026-15115 | Insufficient validation of untrusted input in WebAppInstalls in Google Chrome on Android prior to 150.0.7871.115 allowed a local attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: High) |
| CVE-2026-56372 | ImageMagick before 7.1.2-19 contains a heap buffer overflow vulnerability in the magnify operation that allows attackers to read out of bounds memory. An unrecognized magnify:method value triggers an out of bounds read, potentially exposing sensitive information or causing denial of service. |
| CVE-2026-50416 | Exposure of sensitive information to an unauthorized actor in Windows Win32K allows an authorized attacker to disclose information locally. |
| CVE-2026-61858 | ImageMagick before 7.1.2-26 contains a policy bypass vulnerability in the APNG encoder and external delegates due to missing validation checks. Attackers can write files to disallowed paths by bypassing configured policy restrictions through the APNG encoding process. |
| CVE-2026-50419 | Exposure of sensitive information to an unauthorized actor in Windows Kernel allows an authorized attacker to disclose information locally. |
| CVE-2026-56374 | ImageMagick before 7.1.2-19 contains a heap buffer overflow vulnerability in the FTXT encoder due to missing boundary checks when parsing ftxt:format. Remote attackers can trigger an out of bounds read by crafting malicious FTXT image files to cause denial of service or information disclosure. |
| CVE-2026-59715 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.6.16 before 0.10.0, the Socket.IO server is configured with always_connect=True. The ydoc:awareness:update and ydoc:document:leave Socket.IO handlers accepted collaborative-document events without requiring an authenticated user, allowing unauthorized manipulation of document collaboration state. This issue is fixed in version 0.10.0. |
| CVE-2026-59226 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.0 before 0.10.0, execute_automation rehydrated automation owners without rechecking that they were still active or still had features.automations, and check_model_access only enforced private-model grants for the exact user role, allowing deactivated pending users to continue scheduled model execution. This issue is fixed in version 0.10.0. |
| CVE-2026-52841 | Easy!Appointments is a self hosted appointment scheduler. In versions prior to 1.6.0, `Google::oauth` at `application/controllers/Google.php:278` stores its URL-supplied `provider_id` in the session, and `oauth_callback` saves the issued Google OAuth token against that row without checking the caller owns the provider. Any logged-in backend user (admin, provider, or secretary) rebinds a peer provider's Google sync to a Google account they control. The peer's appointments then sync into the attacker's calendar with each customer's name and email attached as attendee data. Version 1.6.0 patches the issue. |
| CVE-2026-59215 | Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.10.0, channel thread parent and reply handling did not bind parent_id to the channel in the URL, allowing an authenticated user to reference a message from another private or DM channel and disclose thread context across channels. This issue is fixed in version 0.10.0. |
| CVE-2026-13232 | Incorrect Authorization vulnerability in Drupal Advanced Content Feedback (aka admin_feedback) allows Forceful Browsing. This issue affects Advanced Content Feedback (aka admin_feedback) versions: from 0.0.0 to 2.8.0. |
| CVE-2026-59180 | Apprise is an open source library which allows you to send a notification to almost all of the most popular notification services available. Prior to 1.11.0, Apprise HTTP-based notification plugins and HTTP attachment and config loaders in apprise/attachment/http.py and apprise/config/http.py follow HTTP redirects by default and resend user-configured auth headers and query parameters on the redirected request, allowing a compromised trusted destination or on-path attacker to receive secrets such as Authorization headers, bearer tokens, custom headers, and service keys. This issue is fixed in version 1.11.0. |
| CVE-2026-14967 | BBOT's `github_workflows` module could be induced to write a downloaded artifact outside its configured output directory: its path-containment check did not resolve `..`, so a crafted `CODE_REPOSITORY` URL could traverse out of the intended folder. The write is bounded to two directory levels above the output location and its target is determined by the operator's configuration, not the attacker. |
| CVE-2026-15605 | A security vulnerability has been detected in wandb 0.25.2.dev1. Affected is the function ArtifactManifestEntry.download in the library wandb/sdk/lib/hashutil.py of the component Artifact Integrity Validation. The manipulation leads to use of weak hash. The attack may be initiated remotely. A high degree of complexity is needed for the attack. The exploitability is told to be difficult. The pull request to fix this issue awaits acceptance. |
| CVE-2026- | Server-Side Request Forgery (SSRF) vulnerability in Drupal Drupal core allows Server Side Request Forgery. This issue affects Drupal core versions: from 0.0.0 to |

| | |
|---|---|
| 55807 | 10.5.12, from 10.6.0 to 10.6.11, from 11.2.0 to 11.2.14, from 11.3.0 to 11.3.12, from 0.0.0 to 11.0.*, from 0.0.0 to 11.1.*. |
| CVE-2026-14966 | BBOT's unarchive module rejects archives containing symlink entries before extraction, but for zip and 7z archives it failed to detect symlinks whose listing carries a DOS-attribute prefix before the unix mode, as produced by legacy versions of p7zip. Such an archive, downloaded and extracted during a scan (for example via filedownload), bypassed the guard and caused an attacker-controlled symlink to be written into the extraction directory. The effect is limited to planting the symlink (its target is not written through), and only hosts using such a legacy p7zip build are affected; current mainline 7-Zip is not. |
| CVE-2026-61874 | filebrowser versions before 2.63.17 fail to normalize paths before querying the share index in DeleteWithPathPrefix, allowing authenticated users to leave stale public shares behind. Attackers can delete a shared directory using a trailing-slash path, then recreate the same directory to expose new contents through the dormant public share URL. |
| CVE-2025-62826 | An Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting') vulnerability [CWE-113] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.4, FortiOS 7.4 all versions, FortiOS 7.2 all versions, FortiProxy 7.6.0 through 7.6.4, FortiProxy 7.4 all versions, FortiProxy 7.2 all versions may allow an attacker able to intercept and modify a user's captive portal authentication request to inject arbitrary headers via crafted HTTP requests. |
| CVE-2026-15690 | A vulnerability was identified in open62541 up to 1.5.5. Affected by this issue is the function responseReadNamespacesArray of the file src/client/ua_client_connect.c of the component Shared Client Library. Such manipulation of the argument Server_NamespaceArray leads to null pointer dereference. The attack can be executed remotely. The attack requires a high level of complexity. The exploitation is known to be difficult. The exploit is publicly available and might be used. The project closed the issue report, stating that this is not the official way to report a security vulnerability. |
| CVE-2026-61870 | ImageMagick before 7.1.2-26 contains a memory leak vulnerability in the VIFF encoder when memory allocation fails. Attackers can trigger allocation failures by processing specially crafted VIFF images to exhaust available memory and cause denial of service. |
| CVE-2026-13151 | GitLab has remediated an issue in GitLab EE affecting all versions from 16.10 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an authenticated user to modify group-level settings beyond their intended permissions due to improper authorization controls. |
| CVE-2026-6352 | GitLab has remediated an issue in GitLab EE affecting all versions from 18.2 before 18.11.7, 19.0 before 19.0.4, and 19.1 before 19.1.2 that under certain conditions could have allowed an authenticated user with auditor-level access to modify compliance violation records due to improper authorization on certain GraphQL operations. |
| CVE-2026-57961 | phpMyFAQ before 4.1.5 contains a potential authenticated path traversal vulnerability in the concatenatePaths() function within src/phpMyFAQ/Export/Pdf/Wrapper.php. A user with FAQ editing privileges can store HTML containing crafted image paths that are processed during PDF generation. The path resolution logic locates the substring "content" within a user-controlled path using strpos(); when "content" is absent, strpos() returns false, which becomes 0 when cast to an integer, preserving the entire attacker-controlled path. This path is later passed to file_get_contents() without canonicalization or root-directory containment validation, which may allow reading of files outside the intended content directory. |
| CVE-2026-61971 | Authorization Bypass Through User-Controlled Key vulnerability in Cozmoslabs User Profile Picture metronet-profile-picture allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects User Profile Picture: from n/a through <= 2.6.3. |
| CVE-2026-53480 | Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper limitation of a pathname to a restricted directory ('path traversal') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized file modification. |
| CVE-2026-52840 | Easy!Appointments is a self hosted appointment scheduler. In versions prior to 1.6.0, `Caldav::connect_to_server` at `application/controllers/Caldav.php:60` hands the request's `caldav_url` to a Guzzle `REPORT` call without scheme or host validation. A logged-in backend user (admin, provider, or secretary) reaches loopback, RFC1918, and link-local hosts on the deployment's network. The Guzzle exception path returns the upstream status code plus ~120 bytes of response body in the JSON `message` field (`Caldav.php:74-78`), so the SSRF is semi-blind. Version 1.6.0 contains a patch. |
| CVE-2026-8800 | Incorrect Authorization vulnerability in Progress MOVEit Transfer (Audit User module). This issue affects MOVEit Transfer: before 2025.0.7, from 2025.1.0 before 2025.1.3. |
| CVE-2026-52838 | Easy!Appointments is a self hosted appointment scheduler. Versions prior to 1.6.0 allow administrators to define a custom "booking disabled" message through the booking settings page. That value is stored in the `disable_booking_message` setting via a rich-text editor and later passed directly to the public `booking_message` view without escaping or sanitization. An authenticated administrator can store HTML or JavaScript in this field, enable disabled-booking mode, and trigger stored XSS in every unauthenticated visitor who opens the public booking page. Version 1.6.0 fixes the issue. |
| CVE-2026-15168 | BLF file parser in Wireshark 4.6.0 to 4.6.6 and 4.4.0 to 4.4.16 allows possible information disclosure |
| CVE-2026-15321 | A vulnerability was found in MyEMS up to 6.4.0. The affected element is the function on_post of the file myems-api/core/svg.py of the component Admin Backend. The manipulation of the argument new_values['data'] results in cross site scripting. The attack can be launched remotely. The exploit has been made public and could be used. Upgrading to version 6.5.0 is sufficient to fix this issue. The patch is identified as 4a97edfbd786c779d0322054833b21ddf54d5b06. It is suggested to upgrade the affected component. The issue report remains open even though there is an official fix for it. |
| CVE-2026-15532 | A vulnerability was identified in SourceCodester Online Book Store System 1.0. This issue affects some unknown processing of the component User Management Module. Such manipulation of the argument Name/Username leads to cross site scripting. The attack can be executed remotely. The exploit is publicly available and might be used. |
| CVE-2026-10668 | The Nuvoton NuMaker HSUSBD USB device-controller driver (drivers/usb/udc/udc_numaker.c) armed the control Data IN stage unconditionally (base->CEPTXCNT = len in numaker_hsusbd_ep_trigger). Because the HSUSBD hardware cannot disarm a control Data IN already armed for a previous transfer, a USB host that cancels an in-flight control transfer (timeout) and then issues a new SETUP packet can drive the driver out of sync: stale data may be transmitted in the new transfer and the control endpoint can become permanently stuck NAK'ing every subsequent control transfer. A malicious or buggy host (physical/adjacent attacker driving the bus) can repeatedly cancel-and-re-SETUP to wedge the device's USB control endpoint, denying service to the device's USB function (the device stops enumerating/responding on the control pipe) until a USB reset or re-plug. The flaw is an availability-only denial of service; the FIFO copy loops (bounded by net_buf length and the hardware BUFFULL flag) and the net_buf lifecycle are independent of the arming desync, so there is no out-of-bounds access, use-after-free, or information leak. The fix monitors the IN-token and new-SETUP events (k_event) and only arms control Data IN when an IN token is present and no new SETUP has arrived, cancelling the current transfer on a new SETUP. Affects boards using the Nuvoton NuMaker HSUSBD controller (CONFIG_UDC_NUMAKER with DT_HAS_NUVOTON_NUMAKER_HSUSBD_ENABLED); shipped in v4.4.0. |
| CVE-2026-57501 | Zen is a firefox-based browser. Prior to 1.21.5b, Zen's glance and split-view context-menu actions, Open link in glance and Split link in new tab, load a page-controlled link URL with the System principal instead of the originating page's principal, allowing a malicious web page to place a link to a file URL that can load with System privileges when opened through either context-menu item and bypass the content-to-file security check that blocks an ordinary click. This issue is |

| | |
|---|---|
| | fixed in version 1.21.5b. |
| CVE-2026-57480 | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.9.1-alpha.12 and 8.6.82, deeply nested $or, $and, and $nor query condition operators in the REST API or LiveQuery query handling could trigger exponential-time processing in the internal query-traversal helper and block the Node.js event loop. This issue is fixed in versions 9.9.1-alpha.12 and 8.6.82. |
| CVE-2026-15683 | Lorex 2K Indoor Wi-Fi Security Camera Device Management Server Improper Certificate Validation Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Lorex 2K Indoor Wi-Fi Security Cameras. User interaction is not required to exploit this vulnerability. The specific flaw exists within the device management functionality. The issue results from the lack of proper validation of the certificate presented by the server. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-26851. |
| CVE-2026-15684 | Glarysoft Glary Utilities Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Glarysoft Glary Utilities. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Disk Clean functionality. By creating a junction, an attacker can abuse the service to delete arbitrary files. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-27004. |
| CVE-2026-15685 | Ollama downloadBlob Improper Validation of Array Index Denial-of-Service Vulnerability. This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of Ollama. Authentication is not required to exploit this vulnerability. The specific flaw exists within the downloadBlob function. The issue results from the lack of proper validation of user-supplied data, which can result in a memory access past the end of an allocated array. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-27277. |
| CVE-2026-55849 | @cyclonedx/cyclonedx-npm creates CycloneDX Software Bill of Materials from npm projects. From 2.1.0 before 5.0.0, the CLI passes user-supplied --workspace values to a subshell without proper sanitization when npm_execpath is unset or empty, allowing arbitrary OS command execution with the privileges of the invoking user. This issue is fixed in version 5.0.0. |
| CVE-2026-55195 | py7zr is a Python-based library and utility to support 7zip archive compression, decompression, encryption and decryption. Prior to 1.1.3, py7zr's Worker.decompress() extracted archive entries without tracking total decompressed size, allowing a crafted .7z file such as a 15.6 KB archive that expands to 100 MB to exhaust disk or memory before extraction completes. This issue is fixed in version 1.1.3. |
| CVE-2026-58411 | ChurchCRM is an open-source church management system. Prior to version 7.4.0, Cross-Site Scripting (XSS) vulnerabilities were identified due to insufficient output encoding of user-controlled request parameter names and parameter values. The application reflects attacker-controlled input into JavaScript string contexts and HTML attribute contexts without proper sanitization or contextual output encoding. Affected endpoints observed during testing: /FamilyCustomFieldsEditor.php, /PaddleNumList.php and /admin/system/church-info. Potential consequences include session-token theft, account takeover, unauthorized actions on behalf of authenticated users, exposure of sensitive church member information, credential harvesting, phishing, and privilege escalation when administrators are targeted. This issue has been resolved in version 7.4.0. |
| CVE-2026-55471 | HAPI FHIR is a complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. Prior to 6.9.10, org.hl7.fhir.utilities.XsltUtilities saxonTransform(...) overloads instantiated a bare net.sf.saxon.TransformerFactoryImpl() without ACCESS_EXTERNAL_DTD or ACCESS_EXTERNAL_STYLESHEET restrictions, allowing an attacker who controls or can tamper with transformed XML to trigger XML External Entity injection for local file disclosure and blind XXE or SSRF to arbitrary URLs reachable from the host. This issue is fixed in version 6.9.10. |
| CVE-2026-55206 | py7zr is a Python-based library and utility to support 7zip archive compression, decompression, encryption and decryption. Prior to 1.1.3, PackInfo._read() in archiveinfo.py used an O(n^2) cumulative sum pattern for attacker-controlled numstreams values parsed from archive headers, allowing a crafted .7z archive to cause excessive CPU consumption during SevenZipFile.init() before extraction. This issue is fixed in version 1.1.3. |
| CVE-2026-55665 | Grist is spreadsheet software using Python as its formula language. Prior to 1.7.15, Grist contained two cross-site scripting vulnerabilities where an attacker-controlled value reached a link's href without scheme validation, so a javascript URL could run in a victim's Grist origin on a single click. On the account-selection page, /welcome/select-account used its next query parameter as the account buttons' link target. In document tours, the GristDocTour table's Link_URL column became a clickable button, allowing an editor of a shared document to store a javascript URL there that ran when another user opened the document and clicked the tour link. Because the script runs in the victim's authenticated session, it can call Grist APIs as the victim, reading or modifying data and changing sharing settings and access rules. A document editor could therefore escalate to owner-level access. This issue is fixed in version 1.7.15. |
| CVE-2026-55778 | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.9.1-alpha.11 and 8.6.81, the default fileUpload.fileExtensions blocklist could be bypassed by uploading a file with a non-standard or compound extension and dangerous content type, allowing storage adapters such as S3 and GCS to serve attacker-supplied active content and enable stored cross-site scripting. This issue is fixed in versions 9.9.1-alpha.11 and 8.6.81. |
| CVE-2026-55881 | OpenReplay is a self-hosted session replay suite. From 1.22.0 before 1.27.0, getFirstMob returned 15-second presigned S3 download URLs for a session's DOM-replay recording based solely on the session path parameter, while validateProjectAccess checked only that the project belonged to the requester's tenant and did not verify that the session belonged to that project, allowing any authenticated low-privilege user to read another tenant's first 15 seconds of session-replay recording data. This issue is fixed in version 1.27.0. |
| CVE-2026-54527 | JupyterLab Git is a Git extension for JupyterLab. From 0.30.0b3 before 0.54.0, the PlainTextDiff.ts createHeader() method passes Git filenames directly to innerHTML when rendering renamed files in commit history, allowing a crafted filename to execute JavaScript when a victim views the rename diff in the Git History tab. This issue is fixed in version 0.54.0. |
| CVE-2026-57575 | Misskey is an open source, federated social media platform. Prior to 2026.6.0, Misskey contains a Server-Side Request Forgery (SSRF) vulnerability in URL preview functionality in UrlPreviewService. Due to missing network restrictions before establishing outbound connections, a remote attacker can cause the Misskey server to initiate HTTP requests to loopback, private, or link-local services. Because IP address validation takes place after the request has been sent and the process is subsequently rejected, no sensitive internal data is believed to be transmitted back or exposed to the attacker. This issue is fixed in version 2026.6.0. |
| CVE-2026-57574 | Misskey is an open source, federated social media platform. Prior to 2026.6.0, Misskey contains a vulnerability in Time-based One-Time Password (TOTP) authentication in UserAuthService where insufficient validation of used tokens allows the reuse of a single-use code within its valid time step. If both credentials and a TOTP code are obtained concurrently, an attacker may reuse the code to perform unauthorized actions, potentially leading to account takeover. This issue is fixed in version 2026.6.0. |
| CVE-2026-15680 | Lorex 2K Indoor Wi-Fi Security Camera CDeviceOperator Format String Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Lorex 2K Indoor Wi-Fi Security Cameras. Authentication is not required to exploit this vulnerability. The specific flaw exists within the parsing of JSON requests in the sonia binary. The issue results from the lack of proper validation of a user-supplied string before using it as a format specifier. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-25884. |
| CVE-2026-58488 | HedgeDoc is an open source, real-time, collaborative, markdown notes application. Versions prior to 1.11.0 allowed attackers to circumvent the rate-limiting of the /login and /register routes by spoofing IP addresses. HedgeDoc instances checked for CloudFlare's cf-connecting-ip header and used that instead of the users real IP address, if the header was present even when the request did not originate from Cloudflare. This made it possible for an attacker to spam login requests or create multiple arbitrary accounts by sending another cf-connecting-ip header every few requests. The issue has been fixed in version 1.11.0. |
| CVE-2026- | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to 9.9.1-alpha.13 and 8.6.83, a LiveQuery subscriber could receive object field values they were not authorized to read when a single save changed both an object field and the subscriber's ACL read access, because |

| | |
|---|---|
| 57481 | leave and enter events included the wrong object state. This issue is fixed in versions 9.9.1-alpha.13 and 8.6.83. |
| CVE-2026-58487 | HedgeDoc is an open source, real-time, collaborative, markdown notes application. Prior to version 1.11.0, due to unsafe handling of the local-part of registered email addresses, HedgeDoc was vulnerable to stored HTML Injection through its publish and slide views. An attacker could register a specially crafted email address and inject arbitrary HTML into pages viewed by other users. HedgeDoc accepted RFC 5321 quoted-string local-parts in email addresses during registration. The local-part was then reused as the user's display name without escaping and rendered into HTML in multiple places, including publish and slide views as well as the collaborative editor. An attacker could break out of an HTML attribute and inject arbitrary markup into the page. While the deployed Content-Security-Policy prevented straightforward inline JavaScript execution, the injected HTML was still sufficient to alter page content and embed attacker-controlled resources such as cross-origin iframes. This issue was fixed in version 1.11.0. |
| CVE-2026-55884 | Tilt defines dev environments as code for microservice apps on Kubernetes. From 0.20.8 through 0.37.3, the Tilt HUD HTTP server registers handlers on a gorilla/mux router with no authenticating middleware. When the HUD is bound to a non-loopback address, an unauthenticated network caller can trigger developer-defined resources, tamper with Tiltfile arguments, read full engine state including the session token, and invoke apiserver resources through the token-attaching /proxy handler. This issue is fixed in version 0.37.4. |
| CVE-2026-58407 | Rejected reason: Please submit CVE requests for each vulnerability. |
| CVE-2026-56437 | Uncontrolled search path element issue exists in Pupsman versions prior to 3.9.0. If a crafted DLL file is placed in the same folder as the affected installer and the installer is executed, arbitrary code may be executed with SYSTEM privilege. |
| CVE-2026-14286 | Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. |
| CVE-2026-53951 | Copier is a library and CLI app for rendering project templates. In versions 9.5.0 through 9.15.1, the `trust` setting's prefix match (`copier/_settings.py`) compares the template URL against a trusted prefix with a raw `str.startswith` and no path normalization, while the URL is normalized when the template is actually fetched (`Path.resolve()` for local paths; libcurl dot-segment removal for `https`). A template reference that textually starts with a trusted prefix but contains `..` is therefore granted trust yet resolves to a different, attacker-controlled template, whose `tasks` / `migrations` / `jinja_extensions` then run without the `--trust` prompt — arbitrary command execution. Version 9.15.2 patches the issue. |
| CVE-2026-49946 | Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. |
| CVE-2026-49945 | Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. |
| CVE-2026-49944 | Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. |
| CVE-2026-60125 | MISP’s importModule() path used getEnabledModule() to resolve a single import module by name, but this lookup did not enforce the per-organisation module restriction checked by getEnabledModules(). As a result, an authenticated user from an organisation that was not allowed to use a module restricted via Plugin.Import_<module>_restrict could still invoke that import module directly if they knew its name. This could allow unauthorised access to restricted import-module functionality and, depending on the module and the user’s event permissions, may allow unauthorised import or modification of event data through a module that should have been unavailable to the user’s organisation. |
| CVE-2026-60124 | An authorization bypass in MISP’s EventsController::importModule() allowed authenticated users or read-only API keys with event view access to persist data to events they were not allowed to modify. When an import module returned results in the misp_standard format, the write path did not verify event modification rights before saving the module output. This could allow a view-only user to inject or alter event data, impacting the integrity of MISP event content. The issue was fixed by enforcing the same modification-rights check used by related module result handling paths before processing misp_standard imports. |
| CVE-2026-61448 | Parse Server is affected by a stored cross-site scripting (XSS) vulnerability in versions >= 9.0.0, < 9.10.0-alpha.2 and <= 8.6.83. When an uploaded file's extension is not recognized by the mime package, Parse Server preserves the client-supplied Content-Type. A malformed Content-Type that is not a valid type/subtype media type (e.g., 'image', 'image/', or 'image//svg+xml') bypasses the fileUpload.fileExtensions blocklist and is stored unchanged. On storage adapters that persist and serve the uploaded Content-Type (such as Amazon S3, Google Cloud Storage, or Azure Blob Storage), a browser cannot parse the malformed value and falls back to MIME-sniffing; a file whose body begins with HTML is rendered as HTML, executing embedded script in the application's origin against other users who open the file URL. The default GridFS storage adapter is not affected. Fixed in 9.10.0-alpha.2 and 8.6.84. |
| CVE-2026-57895 | Incorrect default permissions issue exists in Pupsman versions prior to 3.9.0. An attacker can place a malicious executable in the installation folder, which results in arbitrary code execution with SYSTEM privilege |
| CVE-2026-62143 | A Server-Side Request Forgery (SSRF) protection bypass existed in the html_to_markdown expansion module of misp-modules. The module attempts to prevent requests to loopback, private, link-local, and other restricted IP address ranges. However, IP addresses were compared against the blocked ranges without first normalising IPv4-mapped IPv6 addresses. An authenticated attacker able to invoke the module could supply an IPv4-mapped IPv6 address, such as: http://[::ffff:127.0.0.1]/ http://[::ffff:169.254.169.254]/ Alternatively, the attacker could use a hostname that resolves to an IPv4-mapped IPv6 address. These addresses were treated as IPv6 addresses and therefore did not match the corresponding blocked IPv4 ranges. Successful exploitation could cause the misp-modules server to connect to services available through its loopback interface, internal network, or link-local network. This could expose internal web services, administrative interfaces, or cloud instance metadata, with retrieved content potentially returned to the attacker as converted Markdown. The vulnerability has been addressed by normalising IPv4-mapped IPv6 addresses to their underlying IPv4 representation before applying the blocked-range checks. URLs without a valid hostname are now also rejected. |
| CVE-2026-58503 | Frappe is a full-stack web application framework. Prior to 16.16.0 and 15.106.0, user enumeration could be performed via the reset_password endpoint. This issue is fixed in versions 16.16.0 and 15.106.0. |
| CVE-2026-13014 | A vulnerability in Thales CERT "Suspicious" application =< 1.3.4 allows a remote and unauthenticated attacker to execute arbitrary code and arbitrarily overwrite writable application files—including Python modules, configuration files, cron inputs, and runtime artifacts—leading to a persistent denial of service, the potential compromise of application secrets or integrations, and root-level execution inside the Django application container. This vulnerability has been names "Matryoshka Mail". Thales PSIRT acknowledges and thanks Lucien Doustaly (aka wlayzz) for discovering and reporting this issue. |

| | |
|---|---|
| CVE-2026-14846 | In version 8.2.1 of PrestaShop, there is a vulnerability relating to the incorrect sanitisation of elements, caused by inadequate validation of the ‘Alias’ parameter in the ‘Update your address’ function. This flaw allows an attacker to inject malicious expressions that are executed when the information is exported using the ‘Get my data in CSV’ tool. Successful exploitation of this vulnerability could facilitate unauthorised access to the victim’s personal data. |
| CVE-2026-22093 | The EVbee Service Android app uses TLS encrypted communication (HTTPS), but does not validate the certificate provided by the server. This allows an attacker on the network path between the app and EVbee server to intercept and manipulate the communication between the app and server. The traffic is weakly encrypted using RC4 with a hardcoded key, which allows an attacker to gain access to the communication. Part of this communication involves access codes to charging stations. This issue affects EVbee Service: v1.4.101.00. |
| CVE-2026-22095 | The network diagnosis endpoint on the web server at port 8090 is vulnerable to command injection. |
| CVE-2026-22096 | The webserver running on port 8090 does not require authentication. This allows for sensitive information leakage such as configured passwords, or uploading files through different endpoints. |
| CVE-2026-22097 | The firmware update mechanism does not include cryptographic signature validation. This allows anyone with access to the firmware update capability to upload arbitrary files which can then lead to arbitrary code execution. |
| CVE-2026-22098 | Various sensitive information such as passwords and charging card UIDs are written to log files. |
| CVE-2026-22099 | The charging station does not require authentication for Bluetooth commands to perform actions. The functionality exposed includes sensitive information leakage, triggering reboots, or pushing a firmware update URL. |
| CVE-2026-22100 | The OCPP DataTransfer message `ReserveLogin` is vulnerable to command injection. By manipulating the data value, arbitrary OS commands can be executed as root. |
| CVE-2026-59155 | Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. Prior to 2.2.5, the GET /api/v1/ddns and GET /api/v1/notification endpoints return full resource objects including plaintext third-party API credentials, including Cloudflare API tokens, TencentCloud SecretKeys, Slack, Discord, and Telegram webhook URLs with embedded bot tokens, and Authorization header values, without any field-level redaction. Any authenticated admin or PAT with nezha:ddns:read or nezha:notification:read scope can receive stored credentials through the listDDNS and listNotification handlers in a single API response. This issue is fixed in version 2.2.5. |
| CVE-2026-57584 | Phalcon is a high-performance, full-stack PHP framework. Prior to 5.15.0, every Phalcon MVC application built with a default router registers a built-in route whose compiled PCRE pattern contains the nested quantifier (/.), and the same construct is produced by the /:params placeholder and the CLI router. Phalcon\Mvc\Router::handle() matches this pattern against the attacker-controlled request URI on every request, so a crafted path such as one containing repeated slashes followed by decoded newlines can trigger catastrophic backtracking and cause CPU exhaustion or route-matching failure. This issue is fixed in version 5.15.0. |
| CVE-2026-6875 | ServiceNow has addressed a remote code execution vulnerability that was identified in the ServiceNow AI platform. This vulnerability could enable an unauthenticated user, in certain circumstances, to execute code within the ServiceNow platform. ServiceNow addressed this vulnerability by deploying a security update to hosted instances. Relevant security updates have also been provided to ServiceNow self-hosted customers and partners. Further, the vulnerability is addressed in the listed patches and family releases, which have been made available to hosted and self-hosted customers, as well as partners. We are not currently aware of exploitation against ServiceNow instances. We recommend customers promptly apply appropriate updates or upgrade to a patched release if they have not already done so. |
| CVE-2026-53364 | In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_conn: Fix memory leak in hci_le_big_terminate() hci_le_big_terminate() allocates iso_list_data via kzalloc_obj but returns 0 without freeing it when neither pa_sync_term nor big_sync_term flags are set after evaluating the PA and BIG sync connection state. This early-return path was introduced when hci_le_big_terminate() was refactored to take struct hci_conn instead of raw u8 parameters, adding PA/BIG flag evaluation logic. The existing kfree() on hci_cmd_sync_queue failure does not cover this path. |
| CVE-2026-58228 | Cross-site scripting vulnerability in phoenixframework phoenix_live_view allows an attacker to bypass URL scheme validation and execute JavaScript in a victim's browser session. The Phoenix.LiveView.Utils.valid_destination!/2 and Phoenix.LiveView.Utils.valid_live_navigation_destination!/2 functions in lib/phoenix_live_view/utils.ex rely on an internal uri_scheme/1 helper that only detects a scheme when the input's first byte is an ASCII letter. Inputs beginning with an ASCII control character or space fall through to a nil-returning clause, causing the URL to be treated as a safe relative path. Standard browsers implement the WHATWG URL parser, which strips leading C0 control and space characters before parsing. As a result, an input such as " javascript:alert(1)" is passed unchanged into <.link href={...}> and, when clicked, is parsed by the browser as a javascript: URL that executes attacker-controlled script in the victim's session. Applications that render user-supplied URLs (for example profile links, redirect targets, or external references) via <.link href={...}> are affected. This issue affects phoenix_live_view: from 1.2.2 before 1.2.7. |
| CVE-2026-41482 | Frappe is a full-stack web application framework. Prior to 16.18.3, possible path traversal and local file inclusion were possible through secure local resource access in the Chrome PDF Generator. This issue is fixed in version 16.18.3. |
| CVE-2026-42219 | Frappe is a full-stack web application framework. Prior to 16.19.0 and 15.109.0, path traversal via download_backups was possible due to lack of hardening. This issue is fixed in versions 16.19.0 and 15.109.0. |
| CVE-2026-47199 | Frappe is a full-stack web application framework. Prior to 16.18.3 and 15.108.0, check_safe_sql_query permitted SELECT INTO OUTFILE queries, which could potentially work on self-hosted sites if database permissions are not well aligned and MySQL FILE privileges are available. This issue is fixed in versions 16.18.3 and 15.108.0. |
| CVE-2026-58212 | Rejected reason: Further research determined the issue is not a vulnerability based on CNA Rule 4.1.12 The act of updating Product dependencies MUST NOT be determined to be a Vulnerability, regardless of whether the dependencies have Vulnerabilities. |
| CVE-2026-47422 | Frappe is a full-stack web application framework. Prior to 15.107.5 and 16.18.2, an endpoint in reportview lacked appropriate permission checks and that has since been fixed. This vulnerability is fixed in 15.107.5 and 16.18.2. |
| CVE-2026- | Frappe is a full-stack web application framework. Prior to 16.20.0 and 15.110.0, users without write access could attach files to any doctype through file-handling API endpoints such as add_attachments. This issue is fixed in versions 16.20.0 and 15.110.0. |

| | |
|---|---|
| 48127 | |
| CVE-2026-55575 | LiquidJS is a Shopify / GitHub Pages compatible template engine in pure JavaScript. Prior to 10.27.1, the pop array filter at src/filters/array.ts allocated a full clone of its input array via [...toArray(v)] without calling this.context.memoryLimit.use(...), allowing a template render such as {{ huge_array \| pop }} to allocate an O(N) clone of an attacker-influenced array outside the configured memoryLimit budget. This issue is fixed in version 10.27.1. |
| CVE-2026-53365 | In the Linux kernel, the following vulnerability has been resolved: vsock/virtio: fix zerocopy completion for multi-skb sends When a large message is fragmented into multiple skbs, the zerocopy uarg is only allocated and attached to the last skb in the loop. Non-final skbs carry pinned user pages with no completion tracking, so the kernel has no way to notify userspace when those pages are safe to reuse. If the loop breaks early the uarg is never allocated at all, leaking pinned pages with no completion notification. Fix this by following the approach used by TCP: allocate the zerocopy uarg (if not provided by the caller) before the send loop and attach it to every skb via skb_zcopy_set(), which takes a reference per skb. Each skb's completion properly decrements the refcount, and the notification only fires after the last skb is freed. On failure, if no data was sent, the uarg is cleanly aborted via net_zcopy_put_abort(). This issue was initially discovered by sashiko while reviewing commit 1cb36e252211 ("vsock/virtio: fix MSG_ZEROCOPY pinned-pages accounting") but was pre-existing. |
| CVE-2026-49394 | Frappe is a full-stack web application framework. Prior to 16.19.0, authorization bypass was possible via the update_page endpoint in Workspace because public workspaces did not receive the required Workspace Manager edit check. This issue is fixed in version 16.19.0. |
| CVE-2026-5923 | Malicious use of a stolen cookie might allow modifications to the contents of the IP phone’s webpage. |
| CVE-2026-61692 | Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-61454. Reason: This candidate is a duplicate of CVE-2026-61454. Notes: All CVE users should reference CVE-2026-61454 instead of this candidate. |
| CVE-2026-6847 | Remote Code Execution vulnerability exists in ThemisNETPanel due to missing authentication for a critical file upload function. The application exposes an endpoint that allows unauthenticated attackers to upload arbitrary PHP files by providing a base64-encoded payload and to execute arbitrary code on the underlying server. This issue has been fixed by a patch released in April 2026. |
| CVE-2026-54736 | Phalcon is a high-performance, full-stack PHP framework. Prior to 5.14.1, Phalcon\Encryption\Crypt::decrypt compares the attacker-supplied HMAC tag against the freshly computed HMAC using PHP/Zephir identity comparison, which lowers to a byte-wise comparison that returns early on the first differing byte. This observable timing discrepancy can allow an attacker to recover a valid tag byte-by-byte and attach it to a chosen IV and ciphertext so that decrypt() accepts tampered encrypted content as authentic. This issue is fixed in version 5.14.1. |
| CVE-2026-12257 | Versions of Mura CMS prior to 10.0.712 contain a critical remote code execution (RCE) vulnerability. The flaw is located in the endpoint “/index.cfm/_api/json/v1/default”, where the “method” parameter in POST requests is not properly validated or sanitised before being processed by the ColdFusion engine. As a result, a remote attacker could exploit this vulnerability to inject and execute arbitrary CFML (ColdFusion Markup Language) expressions and instantiate malicious Java objects, thereby compromising the system’s security. |
| CVE-2026-4765 | Stored Cross-Site Scripting (XSS) vulnerability in the RD Station Conversas chat. The vulnerability resides in the ‘name’ parameter of the initialization process due to improper sanitization of user input. The vulnerability is not limited to self-exploitation: when a support agent joins the conversation, the malicious script also executes in their browser, increasing the impact. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary JavaScript code within the context of the application. |
| CVE-2026-14934 | A Missing Authorization vulnerability in the repository creation functionality in Google Cloud BigQuery, Dataform and Colab Enterprise, in the versions between October 2025 and May 10th, 2026, on Google Cloud Platform, allows an authenticated attacker to escalate privileges and perform cross-tenant repository takeover. This vulnerability was patched on 10 May 2026, and no customer action is needed. |
| CVE-2026-55852 | Frappe is a full-stack web application framework. Prior to 16.23.0 and 15.112.0, TarSlip RCE was possible in Package Import because tarfile members were not sufficiently checked before extraction. This issue is fixed in versions 16.23.0 and 15.112.0. |
| CVE-2026-55882 | Tilt defines dev environments as code for microservice apps on Kubernetes. From 0.19.5 through 0.37.3, the Tilt HUD server mounts Go net/http/pprof handlers under /debug with no access control. When the HUD or apiserver listener is network-exposed, an unauthenticated caller can read process memory through /debug/pprof/heap and /debug/pprof/goroutine, including session and apiserver tokens, and degrade performance through /debug/pprof/profile or /debug/pprof/trace. This issue is fixed in version 0.37.4. |
| CVE-2026-55883 | Tilt defines dev environments as code for microservice apps on Kubernetes. From 0.24.0 through 0.37.3, the Tilt HUD WebSocket at /ws/view is gated by a CSRF token, but the token is served by the unauthenticated /api/websocket_token endpoint and the upgrader accepts clients that omit an Origin header. When the HUD is network-exposed, an attacker who can reach the listener can open the HUD WebSocket and receive the full view stream, including session state, Tiltfile contents, resource statuses, and continued updates. This issue is fixed in version 0.37.4. |
| CVE-2026-5922 | The IP phone might use malicious input stored in configuration parameters and render it as content for the WebUI’s webpage. |
| CVE-2026-22102 | A POST request sent to a specific webserver endpoint can be used to write to arbitrary file locations. The endpoint accepts the filename parameter in the Content-Disposition header without verification. This can be used to cause a denial of service by overwriting system files, or remote-code-execution by overwriting shell-scripts which execution can be triggered through other means. |
| CVE-2026-45756 | Symfony is a PHP framework for web and console applications and a set of reusable PHP components. From 7.3.0-BETA1 until 7.4.12 and 8.0.12, the JsonPath component compiles attacker-controlled match() and search() filter patterns directly into preg_match() without a length cap, i-regexp restriction, or bounded backtracking, allowing catastrophic-backtracking expressions to pin worker CPU and cause denial of service. This issue is fixed in versions 7.4.12 and 8.0.12. |
| CVE-2026-45077 | Symfony is a PHP framework for web and console applications and a set of reusable PHP components. Prior to 5.4.52, 6.4.40, 7.4.12, and 8.0.12, the server:log listener (Symfony\Bridge\Monolog\Command\ServerLogCommand) binds to 0.0.0.0:9911 by default and processes each received frame with unserialize(base64_decode($message)) without authentication, integrity checks, or an allowed_classes allowlist, allowing any reachable host to submit attacker-chosen serialized PHP payloads that can crash the listener and may trigger object-injection gadget effects. This issue is fixed in versions 5.4.52, 6.4.40, 7.4.12, and 8.0.12. |
| CVE-2026-9140 | A denial-of-service security issue exists in the 1719-AENTR. The security issue stems from improper handling of a UDP unicast network storm, which causes the device to become overloaded and lose communication. A power cycle is required to recover. |
| CVE-2026-59855 | SiYuan is an open-source personal knowledge management system. Prior to 3.7.1, Asset.render in app/src/asset/index.ts interpolates the unsanitized this.path value into HTML assigned to innerHTML, allowing a crafted asset link containing a double quote to break out of the src attribute, inject an event handler, and execute JavaScript that can run OS commands in the Electron renderer. This issue is fixed in versions 3.7.1-alpha.2 and 3.7.1. |

| | |
|---|---|
| CVE-2026-9653 | A denial-of-service security issue exists across all the 1756-EN2, EN3, and ENBT communication module due to improper validation of CIP Implicit Connection packets. An attacker on the network can exploit this by sending crafted packets to continuously disrupt device connections, though device connections will recover immediately after. |
| CVE-2026-50180 | Langroid is a framework for building large-language-model-powered applications. Prior to version 0.64.0, `SQLChatAgent` in `langroid` ships a `_validate_query` defense-in-depth layer whose `_DANGEROUS_SQL_PATTERNS` regex blocklist enumerates dangerous SQL primitives by specific function name. The list misses the canonical PostgreSQL filesystem-disclosure family `pg_read_file()`, `pg_stat_file()`, `pg_ls_logdir()`, `pg_ls_waldir()`, `pg_current_logfile()` (and similar `SELECT`-shaped functions in the same family). It also leaves SQL Server `OPENDATASOURCE` and SQLite `ATTACH '<file>' AS x` (DATABASE keyword omitted) unblocked. An attacker able to shape the LLM's generated SQL (directly via prompt input or transitively via prompt-injection in data the LLM ingests) can read arbitrary files from the PostgreSQL host through ordinary `SELECT` queries, even with the agent's strict default configuration (`allow_dangerous_operations=False`, `allowed_statement_types=['SELECT']`). The payloads survive the statement-type allowlist (each is a `SELECT`) and pass through the regex blocklist (none of the function names match), then reach the live SQLAlchemy engine via `SQLChatAgent.run_query`. Version 0.64.0 contains a patch for the issue. |
| CVE-2026-54760 | Langroid is a framework for building large-language-model-powered applications. Prior to version 0.65.1, the `SQLChatAgent` SQL-injection mitigation, with default `allow_dangerous_operations=False`, combines a raw-text regex blocklist (`_DANGEROUS_SQL_PATTERNS`) with a `sqlglot` SELECT-only statement allowlist. The blocklist entries that target callable functions require the function name to be immediately followed by `\s*\(`. PostgreSQL accepts the same call with the name separated from `(` by a quoted identifier, an inline comment, or schema qualification. These forms evade the regex, still parse as `SELECT`, and execute the same PostgreSQL function. This restores the `pg_read_file` server-side file-read primitive that the prior CVE-2026-25879 / GHSA-pmch-g965-grmr fix was meant to block: the parent advisory fixed a missing `pg_read_file` blocklist entry, while this report shows that the added regex is bypassable. Version 0.65.1 fixes the issue. |
| CVE-2026-55615 | Langroid is a framework for building large-language-model-powered applications. Prior to version 0.65.5, Neo4jChatAgent passes LLM-generated Cypher queries straight to the Neo4j driver with no validation, no statement-type allowlist, and no opt-out gate. The query text is influenceable by prompt injection (direct user input or indirect content the agent reads back via RAG), so an attacker who can influence the prompt can read or destroy all graph data and, when APOC or dbms.security procedures are enabled on the server, achieve OS-command and filesystem access. This is the same defect class and threat model as the SQLChatAgent prompt-to-SQL-to-RCE issue fixed in version 0.63.0 (CVE-2026-25879); that fix did not extend to the neo4j module. Version 0.65.5 contains a fix for the neo4j module. |
| CVE-2025-11698 | A denial-of-service issue exists in 5380/5480/5580 controllers boot firmware lower than version 1.072. This vulnerability could potentially allow a malicious user to write invalid file data to the controller, causing the device to enter a major non-recoverable fault (MNRF). |
| CVE-2026-55616 | Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-49757. Reason: This candidate is a duplicate of CVE-2026-49757. Notes: All CVE users should reference CVE-2026-49757 instead of this candidate. |
| CVE-2026-41880 | R-SOFT DMS is vulnerable to OS Command Injection in the Optical Character Recognition (OCR) module. Multiple command execution functions accept user-controllable file paths without proper sanitization before passing them to the system shell via SSH. In current infrastructure the URL encoding neutralizes the injection during the standard web upload flow. An authenticated attacker who is able to trigger the OCR functionality for the uploaded file can execute OS commands within the context of a root user. This issue was fixed in version v3.19-2862 and v3.17-2580. |
| CVE-2026-11403 | A vulnerability in Sonatype Nexus Repository Manager's format-specific API key generation may allow a remote attacker to gain unauthorized access to repository operations as a targeted user. A format-specific API key realm (NuGet API Key, Docker Bearer Token, or npm Bearer Token) must be enabled and the targeted user must have an active API key for this vulnerability to be exploitable. |
| CVE-2026-11917 | A path traversal security issue exists within Rockwell Automation ThinManager® software due to improper limitation of file save operations within the API. An authenticated attacker could exploit this vulnerability to write arbitrary files to restricted system directories outside of the application's intended directory. |
| CVE-2026-41879 | R-SOFT DMS stores superadmin credentials using a non-salted nested MD5 hash. This allows an attacker who obtain password hash to decode superadmin credentials. Critically, this password cannot be changed except by modifying the configuration file. This issue was fixed in version v3.17-2000. |
| CVE-2026-41878 | R-SOFT DMS is vulnerable to Insecure Direct Object Reference (IDOR) attack in multiple file download endpoints. The application fetches files from the database by ID and serves them to whoever requests them, relying only on session authentication, meaning any valid user can access any file. This issue was fixed in version v3.19-2862 and v3.17-2580. |
| CVE-2026-12659 | A denial-of-service security issue exists in the affected products. The security issue stems from improper handling of exceptional conditions when processing crafted CIP packets sent to the adapter. A power cycle is required to recover the module and associated I/O. |
| CVE-2026-41877 | R-SOFT DMS is vulnerable to Stored XSS in file upload functionality. Authenticated attacker can inject arbitrary HTML and JS into the name of the file being uploaded, which will be executed when visiting file list or upload status by other users. This issue was fixed in version v3.19-2832 and v3.17-2580. |
| CVE-2026-59833 | SiYuan is an open-source personal knowledge management system. Prior to 3.7.1, SiYuan renders note and package content to HTML through the Lute engine with sanitization enabled, but Lute's dangerous javascript scheme block does not check form action or SVG xlink:href attributes, allowing stored cross-site scripting in document export-preview and Bazaar package README render paths that can execute OS commands in the Electron desktop renderer. This issue is fixed in versions 3.7.1. |
| CVE-2026-8590 | Vulnerability in Spotfire Spotfire Enterprise (Spotfire Server modules), Spotfire Spotfire Enterprise with External Consumers (Spotfire Server modules), Spotfire Spotfire on Kubernetes (Spotfire Server modules). This issue affects Spotfire Enterprise: through 14.0.12, through 14.4.2, through 14.5.0, through 14.6.1, through 14.6.2, through 14.7.0, through 14.8.0; Spotfire Enterprise with External Consumers: through 14.0.12, through 14.5.0, through 14.6.0, through 14.6.1, through 14.6.2, through 14.7.0, through 14.8.0; Spotfire on Kubernetes: through 4.2.0, 5.0.X, 6.0.X. |
| CVE-2026-14461 | mtr is vulnerable to Out-of-bound read vulnerability in ipinfo_lookup() function. An attacker who can influence the TXT response used for AS lookups can trigger this bug by returning a DNS response that is larger than 512 bytes and uses a crafted compression pointer in the answer NAME field. ipinfo_lookup() function uses the length of the response as the end-of-message boundary for dn_expand() function. The result is a reliable crash. This issue exists in the mtr through version 0.96 and it was fixed in commit 48e1794414d338ce47abc0f27c25ade8788af9c3. |
| CVE-2025-12012 | A denial-of-service issue exists in 5380/5480/5580 controllers. This vulnerability could potentially allow a malicious user to write invalid file data to the controller, causing the device to enter a major non-recoverable fault (MNRF). |
| CVE-2026-8085 | A security issue exists within Arena® Simulation due to a memory corruption vulnerability in the model.exe (Siman) component. The vulnerability stems from improper validation of user-supplied data, which can result in an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process by convincing a user to open a malicious file. |

| | |
|---|---|
| CVE-2026-8312 | A security issue exists within Arena® Simulation due to a memory corruption vulnerability in the expmt.exe (Siman) component. The vulnerability stems from improper validation of user-supplied data, which can result in an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process by convincing a user to open a malicious file. |
| CVE-2026-8313 | A security issue exists within Arena® Simulation due to a memory corruption vulnerability in the linker.exe (Siman) component. The vulnerability stems from improper validation of user-supplied data, which can result in an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process by convincing a user to open a malicious file. |
| CVE-2026-8314 | A security issue exists within Arena® Simulation due to a memory corruption vulnerability in the siman.exe (Siman) component. The vulnerability stems from improper validation of user-supplied data, which can result in an out-of-bounds write. An attacker could leverage this vulnerability to execute arbitrary code in the context of the current process by convincing a user to open a malicious file. |
| CVE-2026-53566 | Out-of-bounds read vulnerability in Citrix Citrix Secure Access Client for Windows. This issue affects Citrix Secure Access Client for Windows: before 26.6.1.20. |
| CVE-2025-12011 | A denial-of-service issue exists in  5370/5570 controllers. This vulnerability could potentially allow a remote user to load an invalid project, causing the device to enter a major non-recoverable fault (MNRF). |
| CVE-2026-10573 | A denial-of-service security issue exists in 1734 POINT I/O™ module. The security issue stems from improper handling of crafted CIP messages, which can cause the module to enter a faulted state. A restart is required to recover. |
| CVE-2026-58225 | SQL Injection vulnerability in elixir-ecto postgrex allows an attacker who can influence a LISTEN channel name to inject SQL into the reconnect replay query, causing a denial of service of the notification connection. Postgrex.Notifications sanitizes channel names with quote_channel/1, which doubles double quotes so the name is safe inside a double-quoted identifier. This protects the single-statement LISTEN and UNLISTEN paths. On every (re)connect, however, handle_connect/1 replays all registered channels at once by concatenating their LISTEN statements and wrapping them in a dollar-quoted anonymous code block (DO $$BEGIN ... END$$). quote_channel/1 does not escape the $$ dollar-quote delimiter that opens and closes this block. The listen/3 guards only reject null bytes and names longer than 63 bytes, so a channel name containing $$ passes validation unchanged. Once such a name is embedded, its $$ prematurely terminates the outer dollar-quoted string and PostgreSQL parses the remainder as additional top-level statements. Because handle_connect/1 runs on every (re)connect, the malformed replay query is rejected each time and the notification connection never re-establishes its subscriptions, silently dropping notifications for every channel sharing that connection. An application is affected when it passes untrusted input (for example a tenant or user identifier) as a channel name to Postgrex.Notifications.listen/3. The double-quote doubling prevents forming a fully valid injected statement, so arbitrary SQL execution is not possible, but the corrupted query reliably breaks the shared notification connection for all tenants, resulting in denial of service. This issue affects postgrex: from 0.16.0 before 0.22.3. |
| CVE-2026-10714 | A security issue exists within FactoryTalk® Services Platform (FTSP), allowing an attacker to bypass JWT signature validation during Okta Web Authentication. The vulnerability stems from the application not verifying that the JWT algorithm is configured for RSA, enabling an attacker to set the algorithm to "none" and craft forged tokens. This could allow an authenticated low-privilege user to impersonate any authorized user on the FTSP server, resulting in unauthorized access to system configuration and the ability to grant permissions to other systems protected by FTSP. |
| CVE-2025-12127 | Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage. |
| CVE-2026-56813 | Improper Neutralization of Parameter/Argument Delimiters vulnerability in elixir-plug plug allows an attacker to inject or override HTTP cookie attributes. The Plug.Conn.Cookies.encode/2 function in lib/plug/conn/cookies.ex builds the Set-Cookie response header by interpolating the cookie value and its path, domain, same_site, and extra attributes directly into the header without neutralizing the ';' delimiter that separates cookie attributes. An application that places attacker-controlled data into a cookie value or attribute (for example via Plug.Conn.put_resp_cookie/4 when reflecting a username or preference) lets an attacker inject a ';' to append or override cookie attributes (such as Domain and Path scope, or dropping the Secure and HttpOnly flags), enabling cookie tossing and session fixation. Carriage return, line feed, and null bytes are rejected by Plug.Conn header validation, so HTTP response splitting is not possible, but attribute injection through ';' is not prevented. This issue affects plug: from 0.1.0 before 1.16.6, from 1.17.0 before 1.17.4, from 1.18.0 before 1.18.5, from 1.19.0 before 1.19.5, from 1.20.0 before 1.20.3. |
| CVE-2026-52837 | Easy!Appointments is a self hosted appointment scheduler. In versions up to and including 1.5.2, the booking reschedule view at `/index.php/booking/reschedule/{appointment_hash}` (handled by `Booking::index()`) embeds the entire customer record as inline JavaScript (`const vars = {... "customer_data": {...}, ...}`) without authentication and without field whitelisting. Anyone in possession of the 12-character `appointment_hash` — which appears in plain text in reschedule emails, confirmation page URLs, and operator-side calendar links — can read every column of that customer's row in the `ea_users` table. Version 1.6.0 contains a patch. |
| CVE-2026-56814 | Plug.Parsers.MULTIPART, the multipart request-body parser used to handle file uploads and multipart forms, does not enforce its :length budget against all consumed resources, allowing an unauthenticated remote attacker to cause denial of service. The parser charges the :length limit only for part body bytes; part header bytes are never counted, and a part with an empty body costs zero. Because every part whose Content-Disposition carries a non-empty filename creates a fresh temporary file (via Plug.Upload) and retains a Plug.Upload struct for the duration of the request, an attacker can send a single request composed of many empty-body file parts. Such a request stays well under the configured :length limit (8,000,000 bytes by default) while creating one temporary file per part, leading to inode and disk exhaustion and unbounded memory growth. Any application using Plug.Parsers with the :multipart parser is affected, and no authentication is required, only reachability of a multipart endpoint over HTTP. This vulnerability is associated with program files lib/plug/parsers/multipart.ex and program routines Plug.Parsers.MULTIPART.parse_multipart/2, Plug.Parsers.MULTIPART.parse_multipart_headers/5, Plug.Parsers.MULTIPART.parse_multipart_body/4, and Plug.Parsers.MULTIPART.parse_multipart_file/4. This issue affects plug: from 1.4.0 before 1.16.6, from 1.17.0 before 1.17.4, from 1.18.0 before 1.18.5, from 1.19.0 before 1.19.5, and from 1.20.0 before 1.20.3. |
| CVE-2026-53363 | In the Linux kernel, the following vulnerability has been resolved: xfrm: iptfs: preserve shared-frag marker in iptfs_consume_frags() iptfs_consume_frags() transfers paged fragments from one socket buffer to another but fails to propagate the SKBFL_SHARED_FRAG flag. This is the same class of bug that was fixed in skb_try_coalesce() for CVE-2026-46300: when fragments backed by read-only page-cache pages are merged, the marker indicating their shared nature must be preserved so that ESP can decide correctly whether in-place encryption is safe. Apply the same two-line fix used in skb_try_coalesce() to iptfs_consume_frags(). |
| CVE-2026-14504 | An authorization bypass in Nexus Repository 3's component upload API allowed a user with only read/browse privileges on a Swift, Terraform, or Conda hosted repository to upload arbitrary artifacts, bypassing the intended write-permission check. |
| CVE-2026-21039 | Improper access control in Settings prior to SMR Jul-2026 Release 1 allows local attackers to configure Theft protection settings. |
| CVE-2026- | Improper access control in IAFDService prior to SMR Jul-2026 Release 1 allows local privileged attackers to use the privileged APIs. |

| | |
|---|---|
| 21040 | |
| CVE-2026-9636 | A security issue exists within CompactLogix® 5380, ControlLogix® 5580, and EN4 communication modules related to CIP Security certificate revocation handling. The security issue stems from the controller failing to properly reject certificates signed by an intermediate certificate that has been revoked via a Certificate Revocation List (CRL). This could allow a network-based attacker to establish a connection using a certificate that should be untrusted, potentially bypassing CIP Security protections. |
| CVE-2026-58461 | Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. |
| CVE-2026-15429 | A privilege escalation vulnerability exists in the HTTP authentication component in Archer VX1800v v1. Improper handling of user-controlled input may allow newline characters to be injected into internally constructed configuration data.  An authenticated user with sufficient privileges may be able to modify account settings and gain elevated administrative privileges. |
| CVE-2026-15428 | An OS command injection vulnerability exists in Archer VX800v v1 due to insufficient input sanitization of the domain name parameter. An adjacent attacker who can access the relevant HTTP interface can modify the parameter to inject shell metacharacters, resulting in arbitrary code execution with root privileges. Successful exploitation may allow remote code execution and complete compromise of the device. |
| CVE-2026-15427 | An OS command injection vulnerability exists in the TR-069 / CWMP management interface of Archer VX1800v v1 due to insufficient input validation and sanitization of parameters, allowing crafted input to be executed as system-level commands. Exploitation requires specific conditions such as TR-069 being enabled and ability to influence ACS-delivered commands, compromise or control an ACS server. Successful exploitation may allow arbitrary command execution with root privileges, resulting in complete compromise of the device. |
| CVE-2026-14646 | Nexus Repository 3 did not apply its existing Server-Side Request Forgery (SSRF) protections to HTTP redirect targets returned by proxy repository upstream servers. Any user with read access to a proxy repository backed by an attacker-controlled or compromised upstream server — including an anonymous user, if anonymous access is enabled — could receive a response from an internal network address or cloud metadata endpoint as repository content, potentially exposing sensitive information such as cloud IAM credentials. |
| CVE-2026-14645 | Nexus Repository 3 does not validate the destination of the "Webhook: Global" capability's configured URL before making an outbound HTTP request, allowing a user holding the Capability Administration permission to cause the server to send requests to internal network locations (Server-Side Request Forgery). This permission is granted by role assignment, independent of authentication status, so an unauthenticated user could also trigger this behavior if the anonymous role has been granted the permission. |
| CVE-2026-9292 | A Stored Cross-Site Scripting security issue exists within FactoryTalk® DataMosaix™ Private Cloud. The vulnerability stems from improper neutralization of user-supplied input within the Workflows configuration. An authenticated attacker with high privileges can inject malicious scripts that are permanently stored on the server. This vulnerability can result in the execution of malicious JavaScript when other users access the affected page, potentially allowing for account takeover, credential theft, or redirection to a malicious website. |
| CVE-2026-21055 | Improper export of android application components in Bixby prior to version 4.0.70.8 allows local attackers to execute arbitrary commands with Bixby privilege. |
| CVE-2026-9128 | A code execution security issue exists within Studio 5000 Logix Designer® due to an unquoted search path in the External Tools configuration. The executable paths specified in the external tools configuration file are not properly quoted, and because these paths contain spaces, the operating system may resolve them to unintended executables placed earlier in the search order. If exploited, an attacker could plant a malicious executable in a location within the search path, resulting in arbitrary code execution with the same permissions of the user running the application. |
| CVE-2026-9127 | A remote code execution security issue exists within Studio 5000 Logix Designer® due to incorrect authorization on a configuration file. This can allow any authenticated user to modify the paths of external tools configured within the application. If exploited, an attacker could alter the configuration to point to a malicious executable, resulting in arbitrary code execution when any user interacts with the external tools functionality. |
| CVE-2026-9108 | A path traversal security issue exists within Studio 5000 Logix Designer® due to improper limitation of file paths within ACD project files. The software does not sanitize or validate file names embedded in the ACD file structure during the project opening procedure, allowing path traversal sequences to escape the intended extraction directory. If exploited, an attacker could craft a malicious ACD project file that results in arbitrary files being written to attacker-controlled locations on the file system, potentially leading to code execution. |
| CVE-2026-7494 | Nexus Repository 3 is vulnerable to Server-Side Request Forgery (SSRF) via the SSL Certificate Retrieval endpoint. A user holding the nexus:ssl-truststore:read permission could cause the server to initiate outbound connections to internal or otherwise restricted network hosts. This issue affects Nexus Repository 3.0.0 through versions prior to 3.94.0. |
| CVE-2026-21057 | Improper input validation in Samsung Pass prior to version 5.2.10.3 allows local privileged attackers to write out-of-bounds memory. |
| CVE-2026-60082 | DBI versions before 1.651 for Perl do not enforce statement handle consistency with the row. When the statement handle had no fields but the source row was non-empty, the internal row-buffer helper would read from a negative array index. This could be triggered by a caller supplying inconsistent metadata and rows to the prepare method. |
| CVE-2026-21056 | Improper authorization in Samsung Health prior to version 7.00.0.107 allows local attackers to access connected device information. |
| CVE-2026-55954 | Authentication Bypass by Spoofing vulnerability in ueberauth ueberauth_apple allows account takeover via unvalidated ID token claims. The Ueberauth.Strategy.Apple.Token.payload/2 function verifies the JWT signature of the callback id_token against Apple's JWKS but does not validate any registered claims. The iss, aud, exp, and iat claims are read from the token and passed on to Ueberauth.Strategy.Apple.handle_callback!/1, which derives the logged-in user's uid and email directly from the unvalidated sub claim. An attacker who obtains any Apple-signed ID token bearing the victim's sub (via a captured expired token, or via an ID token issued to a sibling client in the same Apple developer team) can replay it against the vulnerable callback and be authenticated as the victim. The absent exp check makes stolen tokens usable indefinitely, and the absent aud check enables cross-application account takeover across clients that share an Apple developer team. This issue affects ueberauth_apple: from 0.1.0 before 0.6.2. |
| CVE-2026-21041 | Improper access control in SamsungSEAgentService prior to SMR Jul-2026 Release 1 allows local attackers to access sensitive information. |
| CVE-2026-41876 | R-SOFT DMS is vulnerable to OS Command Injection in konwertujAction() function. The document converter executes shell commands using unsanitized file paths and format parameters. This allows an authenticated attacker to execute arbitrary system commands with the privileges of the web server user. This issue was fixed in version v3.19-2752 and v3.17-2580. |

| | |
|---|---|
| CVE-2026-21042 | Out-of-bounds write in libsavsac.so prior to SMR Jul-2026 Release 1 allows local attackers to execute arbitrary code. |
| CVE-2026-21043 | Path traversal in Wallpaper service prior to SMR Jul-2026 Release 1 allows local privileged attackers to access files with system server privilege. |
| CVE-2026-21044 | Improper authorization in KnoxGuardManager prior to SMR Jul-2026 Release 1 allows local attackers to bypass the persistence configuration of the application. |
| CVE-2026-21045 | Out-of-bounds write in parsing TIFF format in libimagecodec.media.quram.so prior to SMR Jul-2026 Release 1 allows remote attackers to write out-of-bounds memory. |
| CVE-2026-21046 | Time-of-check time-of-use race condition in fabricKeymaster trustlet prior to SMR Jul-2026 Release 1 allows local privileged attackers to execute arbitrary code. |
| CVE-2026-15392 | DBD::File versions before 1.651 for Perl do not ensure the table file is not a symlink to an untrusted location. The complete_table_name method builds the absolute table file path without checking whether the file is a symbolic link. A link inside the data directory can point to a table file at any path outside of the configured f_dir and f_dir_search directories. Callers of file-based drivers can read or write files outside of the data directory. |
| CVE-2026-21048 | Out-of-bounds write in parsing DNG format in libimagecodec.media.quram.so prior to SMR Jul-2026 Release 1 allows remote attackers to write out-of-bounds memory. |
| CVE-2026-21054 | Improper export of android application components in InputSharing prior to version 2.7.01.4 allows local attackers to access sharing data. |
| CVE-2026-21049 | Out-of-bounds write in libpadm.so library prior to SMR Jul-2026 Release 1 allows local attackers to execute arbitrary code. |
| CVE-2026-21050 | Improper access control in SmartThingsKit prior to SMR Jul-2026 Release 1 allows local attackers to access sensitive information. |
| CVE-2026-21051 | Incorrect default permissions in WLAN security prior to SMR Jul-2026 Release 1 allows local attackers to configure TencentWifiSecurity settings. |
| CVE-2026-21052 | Path traversal in SemClipboardService prior to SMR Jul-2026 Release 1 allows local privileged attackers to access files with system privilege. |
| CVE-2026-21053 | Improper input validation in Samsung Email prior to version 6.2.13.1 allows local attackers to create arbitrary files within the application sandbox. |
| CVE-2026-36214 | osTicket versions from 1.10 up to 1.17.7 and from 1.18.0 up to 1.18.3 are vulnerable to a stored XSS due to a vulnerable Bootstrap Tooltip component and insufficient HTML sanitization, allowing remote attackers to execute arbitrary JavaScript in Agent or Admin sessions. |
| CVE-2026-55865 | Python Liquid is a Python engine for the Liquid template language. Prior to 2.2.1, given a malformed {% case %} tag without an associated {% when %} or {% else %} block and no terminating {% endcase %} tag, Python Liquid hangs in an infinite loop at parse time because liquid.TokenStream.eof did not give the EOF token matching kind and value fields, allowing malicious template authors to craft templates for a denial of service attack. This issue is fixed in version 2.2.1. |
| CVE-2026-53565 | Improper Privilege Management vulnerability in Citrix Secure Access Client for Windows, Citrix Citrix Endpoint Analysis Client for Windows. This issue affects Secure Access Client for Windows: before 26.6.1.20; Citrix Endpoint Analysis Client for Windows: before 26. 5.1.7. |
| CVE-2026-15305 | Users were able to upload files with arbitrary MIME types to forms using FileUpload or ImageUpload elements with allowedMimeTypes configured. The restriction was not enforced server-side because the MimeTypeValidator was registered during form building before concrete form definition properties were applied, resulting in the validator never being added to the processing pipeline. This issue affects TYPO3 CMS versions 14.2.0-14.3.5. |
| CVE-2026-55782 | NanaZip is the 7-Zip derivative intended for the modern Windows experience. Prior to 6.5.1749.0, NanaZip's WebAssembly archive handler in NanaZip.Codecs.Archive.WebAssembly.cpp allocates buffers from attacker-controlled 32-bit section and custom-name length fields without validating them against the data present in the file. A tiny crafted module can force multi-gigabyte allocations during listing or extraction through NameSize, Information.Size, and std::string or vector allocation paths, causing memory exhaustion or process termination. This issue is fixed in version 6.5.1749.0. |
| CVE-2026-59161 | Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. Prior to 2.11.0, the streaming worksheet reader used by Rows and GetRows does not enforce the TotalRows limit on the row r attribute, allowing a small XLSX file with a row number above 1048576 and no cell coordinate to make GetRows append empty rows up to the attacker-controlled index and consume excessive memory and CPU. This issue is fixed in version 2.11.0. |
| CVE-2026-50644 | SOPlanning is vulnerable to SQL injection in the audit retention configuration. An attacker holding parameters_all rights can inject SQL commands into the audit configuration form which is then saved. The execution is triggered when the audit functionality is accessed (by the attacker or another user). This issue was fixed in version 1.56.01. |
| CVE-2026-58493 | grav-plugin-database is the database plugin for Grav CMS. Prior to 1.2.0, Database::__call builds PDO DSN strings by directly concatenating user-configurable YAML values from fields such as host, dbname, charset, server, database, directory, and filename without sanitization or validation, allowing an administrator with plugin configuration access to inject DSN attributes or path traversal values. This issue is fixed in version 1.2.0. |
| CVE-2026-58492 | grav-plugin-database is the database plugin for Grav CMS. Prior to 1.2.0, the PDO::tableExists method interpolates its table argument directly into a raw SQL query string without sanitization, escaping, quoting, or whitelisting, allowing attacker-controlled table names passed by consuming plugin or developer code to execute arbitrary SQL against the configured database. This issue is fixed in version 1.2.0. |

| | |
|---|---|
| CVE-2026-57167 | PeerTube is an ActivityPub-federated video streaming platform. Prior to 8.2.2, server-side-rendered video watch pages embed a schema.org JSON-LD block by JSON.stringify-ing video metadata without escaping less-than, greater-than, or slash characters, allowing a value containing the byte sequence that closes a script element to inject arbitrary HTML or JavaScript that executes in the instance origin for visitors to the attacker's videos. This issue is fixed in version 8.2.2. |
| CVE-2026-55783 | NanaZip is the 7-Zip derivative intended for the modern Windows experience. Prior to 6.5.1749.0, NanaZip's seven in-house IInArchive handlers in NanaZip.Codecs unconditionally dereference the caller-supplied Indices array inside Extract when the archive engine signals extract everything by passing Indices as NULL and NumItems as 0xFFFFFFFF. This causes a NULL pointer dereference in the standard Test archive or Extract all code path for WebAssembly, ElectronAsar, Zealfs, Romfs, Ufs, Littlefs, and DotNetSingleFile archives, resulting in a process crash. This issue is fixed in version 6.5.1749.0. |
| CVE-2026-12482 | A vulnerability in keras-team/keras version 3.12.0 allows an attacker to craft a malicious tar archive that bypasses the `filter_safe_tarinfos` validation in `keras/src/utils/file_utils.py`. Specifically, symlink entries are not subjected to the same `is_path_in_dir` validation as regular file entries, allowing symlinks to be created outside the intended extraction directory. This can lead to symlink-based file read, file overwrite, or directory escape attacks. The issue is particularly impactful on Python 3.10 and 3.11, where `filter_safe_tarinfos` is the sole defense against tar path traversal. This vulnerability is distinct from CVE-2025-12060 and other previously reported issues. |
| CVE-2026-60081 | DBI::ProfileData versions before 1.651 for Perl do not limit the path index. The path index column of profile dump files is used to allocate an array of data for the parser. An unbounded value allows an attacker to specify a large index and consume available memory. |
| CVE-2026-55781 | NanaZip is the 7-Zip derivative intended for the modern Windows experience. Prior to 6.5.1749.0, NanaZip's UFS and FFS image handler in NanaZip.Codecs.Archive.Ufs.cpp validates the superblock block size only against the MINBSIZE lower bound and does not validate the fs_fsize fragment size, allowing attacker-controlled 32-bit fields to flow into indirect-block, directory, and extraction buffer allocations. A tiny crafted UFS image can force multi-gigabyte allocations during open or extraction, causing memory exhaustion or process termination. This issue is fixed in version 6.5.1749.0. |
| CVE-2026-55780 | NanaZip is the 7-Zip derivative intended for the modern Windows experience. Prior to 6.5.1749.0, NanaZip's .NET single-file bundle handler in NanaZip.Codecs.Archive.DotNetSingleFile.cpp sizes its extraction buffer from the bundle entry Size field, which is only checked for sign and is not validated against the real file size. A crafted bundle can cause an attacker-chosen allocation inside Extract, where std::bad_alloc or std::length_error can escape across the COM STDMETHODCALLTYPE boundary and crash the process. This issue is fixed in version 6.5.1749.0. |
| CVE-2026-12593 | The implementation of an internal and undocumented Dashboard API endpoint (POST /api/users/~/{user}/tokens) forgot to ensure an HTTP request for creating an API Token for another user had sufficient permission to do so. Precondition for successful exploitation was a preexisting internal user (with more privileges than the attacker), the attacker knowing its login name and the attacker being able to authenticate to the Dashboard via OAuth/OIDC. The attacker would then have had to forge a token creation API request on behalf of the other user and could have authenticated and finalized the token creation with their own OAuth/OIDC credentials. In the worst case, this would mean an attacker could have become Dashboard Administrator and been able to perform all administrative actions if the preexisting internal user had administrative privileges. In combination with a separate weakness, this could have further led to code execution on the host system running the Dashboard with the privileges of the OS-User running the Dashboard server. |
| CVE-2026-12879 | An Improper Input Validation vulnerability in BigQuery DAO in Google Cloud Apigee versions prior to 2026-06-12 on Google Cloud Platform allows an authenticated attacker to exfiltrate cross-tenant data. This vulnerability was patched on 12 June 2026 on the Apigee Servers, and no customer action is needed. |
| CVE-2026-53653 | Grav is a file-based Web platform. Prior to 1.7.53 and 2.0.0-rc.8, Grav allows an unauthenticated visitor to exhaust server memory and CPU by requesting image derivatives with oversized dimensions through URL query image actions such as forceResize in Grav::fallbackUrl, which passes request parameters to ImageMedium magic actions without a dimension or pixel ceiling. This issue is fixed in versions 1.7.53 and 2.0.0-rc.8. |
| CVE-2025-27462 | [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] The Windows PV drivers expose various facilities to userspace. Several of these have no security descriptor, and are therefore fully accessible to unprivileged users. These are: 1. XenCons, CVE-2025-27462 2. XenIface, CVE-2025-27463 3. XenBus, CVE-2025-27464 |
| CVE-2026-59162 | Excelize is a Go language library for reading and writing Microsoft Excel spreadsheets. Prior to 2.11.0, Excelize parses shared-string cell values with strconv.Atoi and checks only the upper bound before indexing the shared string slice, allowing an XLSX file containing a shared-string cell with -1 to trigger sharedStrings[-1] and panic when read through GetCellValue or GetRows. This issue is fixed in version 2.11.0. |
| CVE-2026-59190 | grav-plugin-admin is an HTML user interface that provides a way to configure Grav and create and modify pages. In 1.10.52 and earlier, an authenticated attacker with admin.users permission can change the password of any user account, including the super administrator, by sending a direct POST request to /admin/user/{username}?task=save with data[password] because saveUser authorizes the caller's user-management permission but does not verify whether the caller may edit the target user. This issue is expected to be fixed in version 1.10.53. |
| CVE-2025-27464 | [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] The Windows PV drivers expose various facilities to userspace. Several of these have no security descriptor, and are therefore fully accessible to unprivileged users. These are: 1. XenCons, CVE-2025-27462 2. XenIface, CVE-2025-27463 3. XenBus, CVE-2025-27464 |
| CVE-2026-6872 | Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage. |
| CVE-2026-45074 | Symfony is a PHP framework for web and console applications and a set of reusable PHP components. From 7.1.0 until 7.4.12 and 8.0.12, Cas2Handler builds the CAS service parameter from Request::getSchemeAndHttpHost(), which reflects an attacker-controlled Host header when framework.trusted_hosts is not configured; an attacker controlling another application registered with the same CAS server can replay a victim ticket against the Symfony application and authenticate as the victim. This issue is fixed in versions 7.4.12 and 8.0.12. |
| CVE-2026-45067 | ### Description `Symfony\Component\Mime\Address` is the value-object every Symfony Mailer address (to/cc/bcc/from/reply-to) flows through; its constructor is documented as validating the address and throwing on invalid input, so developers treat it as a security boundary. The constructor accepts email addresses whose local-part (the part before `@`) is an RFC-5322 *quoted string* containing raw `\r\n` bytes — e.g. `"x\r\nBcc: attacker@evil"@example.com`. The stored address is later emitted verbatim into (1) the rendered message headers and (2) `SmtpTransport`'s `MAIL FROM:<...>` / `RCPT TO:<...>` protocol lines, turning the embedded CRLF into a new mail header and/or a new SMTP command. ### Resolution The `Address` constructor now rejects addresses containing line breaks. The patch for this issue is available [here](https://github.com/symfony/symfony/commit/dc2dbd29211eb4ddc451373fa1374fb926e94604) for branch 5.4. ### Credits We would like to thank Claude Mythos Preview (via Project Glasswing) for reporting the issue and providing the fix. |
| CVE-2026-45066 | Symfony is a PHP framework for web and console applications and a set of reusable PHP components. From 6.1.0-BETA1 until 6.4.40, 7.4.12, and 8.0.12, HtmlSanitizer URL sanitization can allow off-allowlist URLs through allowLinkHosts() or allowMediaHosts() because UrlSanitizer::parse() follows RFC 3986 while browsers follow WHATWG URL parsing, and because <area href> is checked against the media policy rather than the link policy. This issue is fixed in versions 6.4.40, 7.4.12, and 8.0.12. |
| CVE-2026- | Symfony is a PHP framework for web and console applications and a set of reusable PHP components. Prior to 5.4.52, 6.4.40, 7.4.12, and 8.0.12, UrlGenerator validates route parameters against a pattern built as ^ plus the raw requirement plus $; with ungrouped alternations, middle alternatives match as unanchored substrings, allowing a value such as //evil.com to satisfy a common locale requirement and generate a protocol-relative off-site URL. This issue is fixed in versions |

| | |
|---|---|
| 45065 | 5.4.52, 6.4.40, 7.4.12, and 8.0.12. |
| CVE-2026-15757 | A security flaw was discovered in the NETGEAR DGND3700v1 that could allow someone on the same local WiFi network to send unauthorized commands to the device. This issue was identified through testing in a controlled research environment using a simulated version of the router's software and has not been confirmed on physical production devices. |
| CVE-2026-15747 | Mojolicious versions from 4.59 before 9.48 for Perl expose a stable representation of the session CSRF token to a BREACH compression oracle. _csrf_token generates and caches one token per session and returns the same value on every call, and _csrf_field places that value in a hidden `csrf_token` input. When a response carrying the token also echoes attacker-controlled input and is gzip-compressed, the chosen values and the resulting compressed lengths form a BREACH oracle. An attacker able to query it can recover the token and pass csrf_protect validation. |
| CVE-2026-41857 | A compromised or malicious BOSH Director can execute arbitrary shell commands on the operator's workstation when the operator runs bosh ssh (or bosh scp/bosh logs -f) with default flags. Affected versions: BOSH CLI versions prior to 7.10.5. |
| CVE-2026-53780 | Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. |
| CVE-2026-58486 | HedgeDoc is an open source, real-time, collaborative, markdown notes application. Prior to version 1.11.0, HedgeDoc was vulnerable to a YAML alias bomb due to unsafe processing of the note frontmatter. HedgeDoc parsed frontmatter with js-yaml.load (js-yaml v3) via @hedgedoc/meta-marked, which resolved YAML anchor aliases. A compact malicious payload could therefore expand into a huge object structure, consuming excessive CPU. This expansion ran on every request to the publish view (/s/<shortid>) and, when placed under the opengraph key, the editor view (/<noteId>). A ten-level alias bomb could block the single Node.js event loop for roughly 235 seconds per request, causing concurrent requests to hang or drop and rendering the instance unavailable (DoS). Because the note was stored in the database, the impact survived process restarts until the note was removed. toobusy-js did not reliably mitigate the worst cases, as the event loop was saturated before the middleware could respond. This issue was fixed in version 1.11.0. |
| CVE-2026-58489 | HedgeDoc is an open source, real-time collaborative markdown notes application. Prior to 1.11.0, the GitHub Gist export flow created an OAuth2 state value but only checked that it was present rather than validating it against the value expected for the user's session. Because the state was not properly validated, an attacker could forge a callback URL containing their own valid GitHub OAuth code. When processing the callback, HedgeDoc used the victim's logged-in session to select which note to export, but the attacker's authorization code to determine which GitHub account received it. As a result, a logged-in victim who clicked a crafted link could export their own private, protected, or limited note directly into a Gist controlled by the attacker. This issue has been fixed in version 1.11.0. |
| CVE-2026-47830 | Incorrect Permission Assignment in BOSH.Utils.psm1 in BOSH-Ecosystem bosh-windows-stemcell-builder allows low-privilege authenticated users to overwrite C:\bosh\service_wrapper.exe or C:\bosh\bosh-agent.exe and gain NT AUTHORITY\SYSTEM on the next service restart or reboot. This can lead to full host control. Affected versions: bosh-windows-stemcell-builder versions prior to v2019.98. |
| CVE-2026-47831 | Use of a cryptographically weak random number generator in the GenerateRandomPassword function in bosh-windows-stemcell-builder allows a remote attacker to brute-force the resulting SSH login via TCP/22. Affected versions: bosh-windows-stemcell-builder versions prior to v2019.98. |
| CVE-2026-55671 | ZITADEL is an open source identity management platform. From 4.0.0-rc.1 through 4.15.1, ZITADEL's HTTP notification channels, OIDC BackChannel Logout, and SAML metadata URL fetches do not consistently validate user-defined URLs against protected denylist handling, allowing server-side requests to loopback, internal IP, link-local, or redirected endpoints through DNS rebinding, redirects, or protocol downgrades. This issue is fixed in version 4.15.2. |
| CVE-2026-55670 | ZITADEL is an open source identity management platform. Prior to 4.15.1, ZITADEL's event store validation can retain the original resource owner for a deleted user identifier, causing a later user recreated with the same identifier in another organization to be provisioned under the original organization and exposed to that organization's administrator. This issue is fixed in version 4.15.2. |
| CVE-2025-27463 | [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] The Windows PV drivers expose various facilities to userspace. Several of these have no security descriptor, and are therefore fully accessible to unprivileged users. These are: 1. XenCons, CVE-2025-27462 2. XenIface, CVE-2025-27463 3. XenBus, CVE-2025-27464 |
| CVE-2025-58146 | There are multiple issues. 1. Updates to the XAPI database sanitise input strings, but try generating the notification using the unsanitised input. This causes the database's event thread to terminate and cease further processing. 2. XAPI's UTF-8 encoder implements v3.0 of the Unicode spec, but XAPI uses libraries which conform to the stricter v3.1 of the Unicode spec. This causes some strings to be accepted as valid UTF-8 by XAPI, but rejected by other libraries in use. Notably, such strings can be entered into the database, after which the database can no longer be loaded. 3. There is no input sanitisation for Map/Set updates on objects in the XAPI database. |
| CVE-2026-12588 | An attacker with access to an HX 10.0.0 and previous versions, may send specially-crafted data to the HX console. The malicious detection would then trigger decompression of a large file that consumes an excessive amount of system resources thus causing a Denial of Service. |
| CVE-2026-54002 | Kirby is an open-source content management system. Prior to 4.9.4 and 5.4.4, Kirby sites and plugins that use the writer or list fields or call Dom::sanitize(), Sane::sanitize(), Sane::Html::sanitize(), Sane::Svg::sanitize(), Sane::Xml::sanitize(), Sane::sanitizeFile(), or file sanitizeContents() with untrusted input allow malicious markup injected as children of an unknown HTML or XML tag to pass through Dom::sanitize() without being correctly sanitized, causing stored cross-site scripting. This issue is fixed in versions 4.9.4 and 5.4.4. |
| CVE-2026-9561 | Eclipse Kura versions prior to 5.6.2 trust the client-supplied X-Forwarded-For HTTP header as the authoritative source of the client IP address in audit log entries. The org.eclipse.kura.web2 (Web Console) and org.eclipse.kura.rest.provider (REST API) components use this header as the primary IP source when initializing audit context, and org.eclipse.kura.jetty.customizer unconditionally installs Jetty's ForwardedRequestCustomizer on all HTTP/HTTPS connectors, causing HttpServletRequest.getRemoteAddr() to reflect the attacker-controlled header value. An unauthenticated remote attacker can exploit this vulnerability to bypass IP-based brute-force protections — such as fail2ban — by spoofing the logged IP address to a non-routable value, allowing a brute-force attack to proceed undetected, or to cause a denial of service against a third party by injecting a victim's IP address and triggering a ban on that address. |
| CVE-2026-14852 | Privilege escalation in Checkmk versions 2.5.0 before 2.5.0p9, 2.4.0 before 2.4.0p34, 2.3.0 before 2.3.0p49, and 2.2.0 (EOL) allows a local unprivileged user to execute arbitrary commands as root by starting a process crafted to look like a SAP HANA instance. Without an explicit database configuration, the mk_sap_hana agent plugin derives instance identifiers from the process list and uses them to build a command executed with elevated privileges (requires the plugin to run as root with RUNAS=agent). |
| CVE-2026-15389 | A vulnerability relating to insufficient access control has been identified in the session management of the Sesame Time web application and its REST v3 API. The flaw lies in the fact that the system uses the session identifier (USID) as the sole validation mechanism, without verifying whether that identifier legitimately belongs to the user making the request. As a result, an attacker who obtains a valid USID can impersonate a victim’s session and access their confidential information, including emails, user IDs, roles and corporate data. This vulnerability is exacerbated by poor session lifecycle management: new logins generate additional USIDs without revoking the previous ones, allowing multiple active sessions to coexist and thereby expanding the attack surface. |
| CVE- | Kirby is an open-source content management system. Prior to 4.9.4 and 5.4.4, Kirby sites using the pages field with roles that have the pages.access permission |

| | |
|---|---|
| 2026-49274 | disabled allowed authenticated users to provide an inaccessible parent page or site to the page picker backend and confirm arbitrary page existence and retrieve title field values. This issue is fixed in versions 4.9.4 and 5.4.4. |
| CVE-2026-49276 | Kirby is an open-source content management system. Prior to 4.9.4 and 5.4.4, Kirby sites using the writer field in any blueprint allowed a scripting link to be included as the target of a link or email link in writer mark components, making the target clickable by the user who entered it and enabling self cross-site scripting in the Panel. This issue is fixed in versions 4.9.4 and 5.4.4. |
| CVE-2026-50188 | Kirby is an open-source content management system. Prior to 4.9.4 and 5.4.4, Kirby sites and plugins using the Kirby Http Remote class, including Remote::request(), Remote::get(), and Remote::post(), to send outgoing HTTP requests with untrusted data in the headers option could allow newline characters in a header value to inject a separate unintended request header to the remote service. This issue is fixed in versions 4.9.4 and 5.4.4. |
| CVE-2026-54003 | Kirby is an open-source content management system. Prior to 4.9.4 and from 5.4.4, Kirby sites with no configured user accounts that run on publicly accessible servers behind a reverse proxy setting the Forwarded, X-Client-IP, or X-Real-IP request header could allow remote attackers to install the Panel and create the first admin user because local-IP checks trusted those headers incorrectly. This issue is fixed in versions 4.9.4 and 5.4.4. |
| CVE-2026-58229 | Allocation of resources without limits vulnerability in elixir-mint mint allows a remote HTTP server to exhaust memory on the client host and cause a denial of service. The Mint.HTTP1.decode_headers/5 and Mint.HTTP1.decode_trailer_headers/4 functions in lib/mint/http1.ex accumulate every parsed response header and chunked-trailer field into a per-request list that persists across incoming TCP segments as request.headers_buffer, and only clear it when the terminating blank line is received. The section has no cap on the number of headers or on total bytes, and the underlying :erlang.decode_packet(:httph_bin, binary, []) parser is invoked with an empty option list so its per-line and per-packet size limits also default to unlimited. A malicious HTTP server (reachable directly, via an attacker-controlled redirect, via SSRF, or via a man-in-the-middle) can stream complete header lines (or, after a chunked body, complete trailer lines) indefinitely without ever emitting the terminating blank line. The connection state grows without bound until the BEAM node is killed by the operating system's out-of-memory handler, taking down the entire application that uses Mint as an HTTP client. This issue affects mint: from 0.1.0 before 1.9.2. |
| CVE-2026-54004 | Kirby is an open-source content management system. Prior to 4.9.4 and 5.4.4, Kirby sites with content.fileRedirects enabled could redirect unauthenticated clean file URL requests for files stored in top-level draft pages to physical media URLs without checking page access permissions or preview tokens, leading to disclosure of draft file contents. This issue is fixed in versions 4.9.4 and 5.4.4. |
| CVE-2026-54005 | Kirby is an open-source content management system. Prior to 4.9.4 and 5.4.4, Kirby sites where a role has the pages.access permission disabled allowed authenticated users who know or guess page IDs or UUIDs to retrieve page information, including full content and metadata, for arbitrary published pages through the /api/site/find route without authorization to access those pages. This issue is fixed in versions 4.9.4 and 5.4.4. |
| CVE-2026-0276 | A privilege escalation vulnerability in Palo Alto Networks Cortex® XDR Broker VM enables a locally authenticated user to perform actions as the root user. |
| CVE-2026-10577 | A security issue exists within the 1715-AENTR EtherNet/IP Adapter. The affected product exposes a network-accessible debug port that does not enforce proper privilege controls, allowing unauthenticated remote access to intrusive command-line interface (CLI) commands. If exploited, a threat actor could read or delete files, stop tasks, modify memory, and change I/O states, potentially impacting the confidentiality, integrity, and availability of the device. |
| CVE-2026-0277 | An improper certificate validation vulnerability in the Prisma® Access Agent for iOS enables an attacker to perform a man-in-the-middle (MitM) attack to intercept VPN traffic. The Prisma Access Agent on Windows, macOS, Linux, Android and ChromeOS are not affected. |
| CVE-2026-0278 | Multiple protection mechanism failures in the Prisma Access Agent Data Loss Prevention (DLP) component for Windows allow a local user to bypass DLP policy enforcement controls. The Prisma Access Agent on macOS is not affected. |
| CVE-2026-59246 | Allocation of resources without limits vulnerability in elixir-mint mint allows a remote HTTP/2 server to exhaust memory on the client host and cause a denial of service. The Mint.HTTP2.handle_continuation/3 function in lib/mint/http2.ex accumulates the header-block fragment carried by each HTTP/2 CONTINUATION frame into a growing conn.headers_being_processed nesting, one level deeper per frame, and only releases it when a frame with the END_HEADERS flag arrives. The only guard on this accumulator is Mint.HTTP2.assert_header_block_within_max_size/2, which sums the byte size of the fragments received so far. Because a CONTINUATION frame is permitted by the protocol to carry a zero-length payload, an unbounded chain of zero-length CONTINUATION frames adds no bytes to the running total, never trips the size cap, and never emits END_HEADERS, yet each frame still nests the accumulator one level deeper. A malicious HTTP/2 server (reachable directly, via an attacker-controlled redirect, via SSRF, or via a man-in-the-middle) can open a stream by sending a HEADERS frame without END_HEADERS and then stream zero-length CONTINUATION frames indefinitely. Client memory grows one cons cell per frame received; sustained bandwidth from the peer drives the BEAM node running the Mint client to memory exhaustion and eventual out-of-memory termination. This issue affects mint: from 0.1.0 before 1.9.2. |
| CVE-2026-15183 | Multiple input validation vulnerabilities in the Snowflake Spark Connector (spark-snowflake) versions prior to 3.2.1 can allow attackers to exfiltrate OAuth client credentials, execute arbitrary SQL with the connector's Snowflake role, or redirect COPY operations to attacker-controlled storage. An attacker could exploit these vulnerabilities by supplying a crafted OAuth token request URL, placing malicious files in an ingestion pipeline, injecting SQL via staging options in a shared Spark environment , or issuing runtime SET commands in a shared Spark-SQL session to inject arbitrary SQL into the SnowflakeFallbackCatalog's option map, which executes under the cluster admin's JDBC credentials. Successful exploitation may result in credential theft, unauthorized access to Snowflake account data, or privilege escalation within connected infrastructure. |
| CVE-2025-58151 | varstored is a component of the Xapi toolstack handling UEFI Variables for a VM. It has a communication path with OVMF inside the VM involving mapping a buffer prepared by OVMF. Within varstored, there were insufficient compiler barriers, creating TOCTOU issues with data in the shared buffer. The exact vulnerable behaviour depends on the code generated by the compiler. In a build of varstored using default settings, the attacker can control an index used in a jump table. |
| CVE-2026-42486 | [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] XAPI can configure different users with different roles, using Role Based Access Control. For more details, see: https://docs.xenserver.com/en-us/xencenter/current-release/rbac-overview.html#rbac-roles The pool-admin role is fully privileged. Notably, users with this role can also SSH into the host as root. The other administrator roles are pool-operator, vm-power-admin and vm-admin, each of which are authorised to configure and manage various aspects of the system. Some settings are inadequately restricted, and can be set by a lower privilege of administrator than expected. * CVE-2026-23559: A vm-admin can set VBD.other_config:backend-local and turn arbitrary files in dom0 into VDIs (virtual disks) and give said disks to a VM they control. This is an arbitrary read and/or modify of files in dom0. * CVE-2026-23560: A vm-admin can set VM.other-config:is_system_domain and mark a VM as a system domain. System domains are ignored and left running during certain other host/pool operations, and may be hidden from view in tooling. * CVE-2026-23561: A vm-admin can set VM.other_config:storage_driver_domain and mark a VM as the storage domain for a particular host storage connection (PBD). Shutting down the VM can cause the PBD to be erroneously marked as unplugged when it is not. * CVE-2026-23562: Configuration of PCI passthrough is normally restricted to the pool-admin role. However one API was missing this check, allowing a vm-admin access to unintended host hardware. * CVE-2026-42486: A vm-admin can set the VM.platform:hvm_serial parameter, which should be restricted to the pool-admin role, as it can allow arbitrary dom0 file write. |
| CVE-2026-54001 | osquery is a SQL powered operating system instrumentation, monitoring, and analytics framework. Prior to 5.23.1, on Windows, a local unprivileged attacker can cause a heap buffer out-of-bounds write if there is a query of the authenticode table targeting a maliciously crafted binary, due to publisher information parsing in getOriginalProgramName. If exploited successfully, this could allow a potential local privilege escalation from standard user to SYSTEM. This issue is fixed in version 5.23.1. |

| | |
|---|---|
| CVE-2026-23556 | When oxenstored is tearing a domain down, the node data is cleaned up but the usage counts are leaked. When the domain ID is eventually reused, the new domain can create fewer nodes before beeing deemed to be over quota. |
| CVE-2026-23559 | [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] XAPI can configure different users with different roles, using Role Based Access Control. For more details, see: https://docs.xenserver.com/en-us/xencenter/current-release/rbac-overview.html#rbac-roles The pool-admin role is fully privileged. Notably, users with this role can also SSH into the host as root. The other administrator roles are pool-operator, vm-power-admin and vm-admin, each of which are authorised to configure and manage various aspects of the system. Some settings are inadequately restricted, and can be set by a lower privilege of administrator than expected. * CVE-2026-23559: A vm-admin can set VBD.other_config:backend-local and turn arbitrary files in dom0 into VDIs (virtual disks) and give said disks to a VM they control. This is an arbitrary read and/or modify of files in dom0. * CVE-2026-23560: A vm-admin can set VM.other-config:is_system_domain and mark a VM as a system domain. System domains are ignored and left running during certain other host/pool operations, and may be hidden from view in tooling. * CVE-2026-23561: A vm-admin can set VM.other_config:storage_driver_domain and mark a VM as the storage domain for a particular host storage connection (PBD). Shutting down the VM can cause the PBD to be erroneously marked as unplugged when it is not. * CVE-2026-23562: Configuration of PCI passthrough is normally restricted to the pool-admin role. However one API was missing this check, allowing a vm-admin access to unintended host hardware. * CVE-2026-42486: A vm-admin can set the VM.platform:hvm_serial parameter, which should be restricted to the pool-admin role, as it can allow arbitrary dom0 file write. |
| CVE-2026-23560 | [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] XAPI can configure different users with different roles, using Role Based Access Control. For more details, see: https://docs.xenserver.com/en-us/xencenter/current-release/rbac-overview.html#rbac-roles The pool-admin role is fully privileged. Notably, users with this role can also SSH into the host as root. The other administrator roles are pool-operator, vm-power-admin and vm-admin, each of which are authorised to configure and manage various aspects of the system. Some settings are inadequately restricted, and can be set by a lower privilege of administrator than expected. * CVE-2026-23559: A vm-admin can set VBD.other_config:backend-local and turn arbitrary files in dom0 into VDIs (virtual disks) and give said disks to a VM they control. This is an arbitrary read and/or modify of files in dom0. * CVE-2026-23560: A vm-admin can set VM.other-config:is_system_domain and mark a VM as a system domain. System domains are ignored and left running during certain other host/pool operations, and may be hidden from view in tooling. * CVE-2026-23561: A vm-admin can set VM.other_config:storage_driver_domain and mark a VM as the storage domain for a particular host storage connection (PBD). Shutting down the VM can cause the PBD to be erroneously marked as unplugged when it is not. * CVE-2026-23562: Configuration of PCI passthrough is normally restricted to the pool-admin role. However one API was missing this check, allowing a vm-admin access to unintended host hardware. * CVE-2026-42486: A vm-admin can set the VM.platform:hvm_serial parameter, which should be restricted to the pool-admin role, as it can allow arbitrary dom0 file write. |
| CVE-2026-23561 | [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] XAPI can configure different users with different roles, using Role Based Access Control. For more details, see: https://docs.xenserver.com/en-us/xencenter/current-release/rbac-overview.html#rbac-roles The pool-admin role is fully privileged. Notably, users with this role can also SSH into the host as root. The other administrator roles are pool-operator, vm-power-admin and vm-admin, each of which are authorised to configure and manage various aspects of the system. Some settings are inadequately restricted, and can be set by a lower privilege of administrator than expected. * CVE-2026-23559: A vm-admin can set VBD.other_config:backend-local and turn arbitrary files in dom0 into VDIs (virtual disks) and give said disks to a VM they control. This is an arbitrary read and/or modify of files in dom0. * CVE-2026-23560: A vm-admin can set VM.other-config:is_system_domain and mark a VM as a system domain. System domains are ignored and left running during certain other host/pool operations, and may be hidden from view in tooling. * CVE-2026-23561: A vm-admin can set VM.other_config:storage_driver_domain and mark a VM as the storage domain for a particular host storage connection (PBD). Shutting down the VM can cause the PBD to be erroneously marked as unplugged when it is not. * CVE-2026-23562: Configuration of PCI passthrough is normally restricted to the pool-admin role. However one API was missing this check, allowing a vm-admin access to unintended host hardware. * CVE-2026-42486: A vm-admin can set the VM.platform:hvm_serial parameter, which should be restricted to the pool-admin role, as it can allow arbitrary dom0 file write. |
| CVE-2026-23562 | [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] XAPI can configure different users with different roles, using Role Based Access Control. For more details, see: https://docs.xenserver.com/en-us/xencenter/current-release/rbac-overview.html#rbac-roles The pool-admin role is fully privileged. Notably, users with this role can also SSH into the host as root. The other administrator roles are pool-operator, vm-power-admin and vm-admin, each of which are authorised to configure and manage various aspects of the system. Some settings are inadequately restricted, and can be set by a lower privilege of administrator than expected. * CVE-2026-23559: A vm-admin can set VBD.other_config:backend-local and turn arbitrary files in dom0 into VDIs (virtual disks) and give said disks to a VM they control. This is an arbitrary read and/or modify of files in dom0. * CVE-2026-23560: A vm-admin can set VM.other-config:is_system_domain and mark a VM as a system domain. System domains are ignored and left running during certain other host/pool operations, and may be hidden from view in tooling. * CVE-2026-23561: A vm-admin can set VM.other_config:storage_driver_domain and mark a VM as the storage domain for a particular host storage connection (PBD). Shutting down the VM can cause the PBD to be erroneously marked as unplugged when it is not. * CVE-2026-23562: Configuration of PCI passthrough is normally restricted to the pool-admin role. However one API was missing this check, allowing a vm-admin access to unintended host hardware. * CVE-2026-42486: A vm-admin can set the VM.platform:hvm_serial parameter, which should be restricted to the pool-admin role, as it can allow arbitrary dom0 file write. |
| CVE-2026-58125 | Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. |
| CVE-2026-14278 | Rejected reason: After further coordination, CVE was determined to not be warranted. |
| CVE-2026-61474 | An improper authorization check in MISP’s attribute creation endpoint allowed an authenticated user with permission to add attributes to submit a sharing_group_id without triggering the corresponding sharing group authorization check, as long as the attribute distribution value was not explicitly set to 4 — “sharing group”. As a result, a user could reference or associate an attribute with a sharing group they were not authorized to use. This could lead to an access-control bypass affecting the integrity of attribute sharing metadata and potentially expose or misuse restricted sharing group relationships. The patch changes the authorization logic so that the sharing group permission check is performed whenever a non-empty sharing_group_id is provided, regardless of the selected distribution value. |
| CVE-2026-59674 | A UNIX Symbolic Link (Symlink) Following vulnerability in openSUSE Tumbleweed suricata package allows the suricata user to escalate to root. This issue affects openSUSE Tumbleweed: from ? before 8.0.5-2.1; openSUSE Tumbleweed: from ? before 8.0.5-2.1. |
| CVE-2026-6851 | An Improper link resolution before file access ('link following') vulnerability in the File Shredder module as used in Bitdefender Total Security and Internet Security on Windows allows a less-privileged local user to elevate rights by leveraging a race conditions via Symbolic Links. This issue affects Total Security: before 27.0.58.315; Internet Security: before 27.0.58.315. |
| CVE-2026-54000 | osquery is a SQL powered operating system instrumentation, monitoring, and analytics framework. Prior to 5.23.1, on Windows, a local unprivileged attacker can cause a heap buffer out-of-bounds write if there is a query of the processes table targeting a maliciously crafted process, due to unchecked PEB string lengths in process command-line and current-directory reads. If exploited successfully, this could allow a potential local privilege escalation from standard user to SYSTEM. This issue is fixed in version 5.23.1. |
| CVE-2025- | A Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in SUSE Virtual Machine Driver Pack allows an attacker with the ability to modify the registry to affect the integrity of the driver. We're not aware of a feasible way to exploit this currently. This issue affects Virtual Machine Driver Pack: |

| | |
|---|---|
| 8412 | before e7a602ec232756ead019bdf19d6d3b9d010cc94b. |
| CVE-2026-54058 | Pillow is a Python imaging library. Prior to 12.3.0, when Pillow loads an uncompressed McIdas AREA image from a filename through the mmap raw codec path, attacker-controlled header words can set a row stride smaller than the natural row width, causing pixel access such as Image.tobytes(), getpixel, convert, or save to read beyond the mapped region and disclose adjacent process memory or fault. This issue is fixed in version 12.3.0. |
| CVE-2026-22103 | The NPC start endpoint on the web server at port 8090 is vulnerable to command injection. |